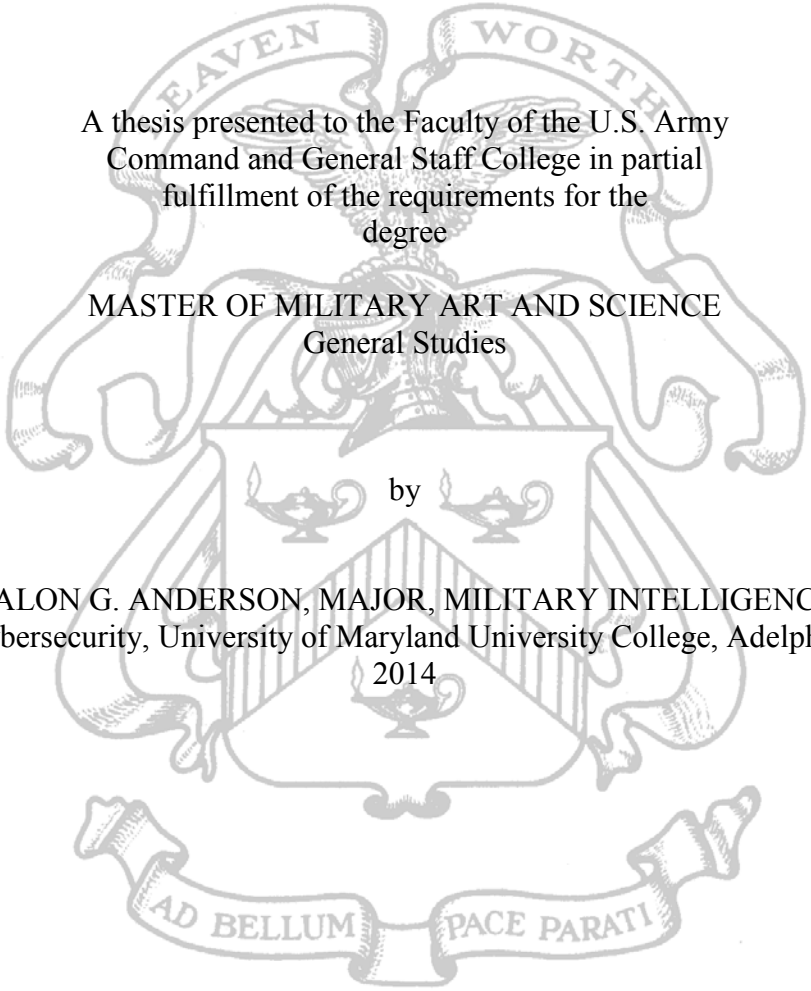
ADAPTING UNCONVENTIONAL WARFARE DOCTRINE TO CYBERSPACE OPERATIONS: AN EXAMINATION OF HACKTIVIST BASED INSURGENCIES



A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

TALON G. ANDERSON, MAJOR, MILITARY INTELLIGENCE
Master of Cybersecurity, University of Maryland University College, Adelphi, Maryland, 2014

Fort Leavenworth, Kansas
2015

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-06-2015	Master's Thesis	AUG 2014 – JUNE 2015

4. TITLE AND SUBTITLE

Adapting Unconventional Warfare Doctrine to Cyberspace Operations: An Examination of Hacktivist Based Insurgencies

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Talon Anderson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study proposes how cyberspace operations can best support online resistance movements to influence adversary national will or affect political behavior to achieve U.S. strategic objectives. Political and social hacker activists (hacktivists) are disrupting governments, organizations, companies, and influencing popular and social movements to achieve their causes. Within the cyber domain, technically-capable, socially-aware guerilla-type hacktivists struggle against governments in ways similar to unconventional warfare (UW) campaigns in physical domains. There is currently a gap between UW and cyberspace operations on how best to properly engage, support, and organize an insurgency in cyberspace. Current conditions on the Internet present an opportunity to implement UW within a new domain through online resistance groups and organizations, specifically with the use of hacktivists. An analysis of the Hong Kong Umbrella Revolution of 2014 validates the potential for a UW campaign using a proposed six-phased cyberspace UW model.

15. SUBJECT TERMS

Unconventional Warfare, Cyberspace Operations, Cyber Warfare, Hacktivism, China, Russia, Georgia, Estonia, Umbrella Revolution, UW, Cyber, Guerilla, Hacktivist, Cyber Domain

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	91	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Talon G. Anderson

Thesis Title: Adapting Unconventional Warfare Doctrine to Cyberspace Operations: An Examination of Hacktivist Based Insurgencies

Approved by:

_____, Thesis Committee Chair
Daniel A. Gilewitch, Ph.D.

_____, Member
LTC David M. Bresser, M.S.

_____, Member
CW3 Ari Jean-Baptiste, M.A.

_____, Member
LTC Paul M. Zeps, M.S.

Accepted this 12th day of June 2015 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

ADAPTING UNCONVENTIONAL WARFARE DOCTRINE TO CYBERSPACE OPERATIONS: AN EXAMINATION OF HACKTIVIST BASED INSURGENCIES, by Major Talon Anderson, 91 pages.

This study proposes how cyberspace operations can best support online resistance movements to influence adversary national will or affect political behavior to achieve U.S. strategic objectives. Political and social hacker activists (hacktivists) are disrupting governments, organizations, companies, and influencing popular and social movements to achieve their causes. Within the cyber domain, technically-capable, socially-aware guerilla-type hacktivists struggle against governments in ways similar to unconventional warfare (UW) campaigns in physical domains. There is currently a gap between UW and cyberspace operations on how best to properly engage, support, and organize an insurgency in cyberspace. Current conditions on the Internet present an opportunity to implement UW within a new domain through online resistance groups and organizations, specifically with the use of hacktivists. An analysis of the Hong Kong Umbrella Revolution of 2014 validates the potential for a UW campaign using a proposed six-phased cyberspace UW model.

ACKNOWLEDGMENTS

This study was done with the great support of Dr. Gilewitch, LTC Zeps, LTC Bresser, and CW3 Jean-Baptiste. Thank you, gentlemen, for your help in this cause, and for finding interest in the subject. It was a long road. Thank you also for believing that the topic was a good idea; time will tell if it was written well enough to be convincing.

Additional help was provided by Mr. Rusty Rafferty whose extraordinary research skills saved dozens of hours in the beginning, and who continued to send articles of interest throughout the entire process. Thank you for considering me. I would also like to thank COL Michael Gilmer (Ret.) for his time reading through this document, identifying its copious grammatical errors, and still remaining positive.

Finally, I would like to thank my wife for putting up with me while writing this effort. She was supportive at all times, and cheerfully acted interested when I engaged her on the topic. No one could ask for a better wife.

TABLE OF CONTENTS

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> The march of science suggests the next war will employ many new means. In contrast, history suggests that by its very nature, war exhibits many continuities amid change.
>
> — Robert F. Baumann, *Historical Perspectives on Future War*

War in a New Domain

The United States wages a bloodless war every day, costing our nation billions of dollars annually as we struggle to defend and deter relentless attack. The nature of conflict has evolved rapidly in a short span of years, and the U.S. must quickly adapt to meet the challenge. For the first time since the end of World War II (or perhaps later when considering the domain of Space), the operational environment now includes a new domain; a domain in which the world's nation-states constantly struggle for dominance. A new kind of conflict has emerged within the domain of cyberspace that impacts social, political and military activities.

Military historians predicted that changes in information technology would affect military affairs in the twenty-first century, but they also cautioned that previous revolutionary elements found their greatest influence from society and politics (Knox and Murray 2001). The Internet revolution has proven its impact on societies. Social media and personal electronic devices have enabled individuals to flock together in like-minded groups unlike any other time in history, reaching audiences on a global scale with unparalleled immediacy. This has given rise to the technically-savvy political activist hacker and ultimately–hacktivism.

It is in this new domain, that an army of technically-capable and socially-aware hacktivists transform themselves into new actors influencing businesses, governments and cultures. For the U.S. Armed Forces to stay relevant and capable of supporting strategic end states, it must develop methods to influence, counter or support these hacktivists, thus enabling the free flow of information across the Internet and the shift of adversarial governments' policies in favor individual freedoms.

This study examines a gap within U.S. military activities surrounding online organizations and cyberspace operations. The fundamental application of cyberspace operations in U.S. doctrine does not currently include a discussion on how to support a population in pursuit of political goals and individual freedoms. These pursuits are critical elements in the debate for access to information through the Internet in the world today. The policies and activities of the U.S. should be evaluated to determine applicability in this new domain for online groups, organizations and personas on the internet, and whether current conditions represent opportunities for the U.S. to adapt and meet future challenges.

The Problem

The U.S. requires a concept on how best to implement cyberspace operations to meet the demands of an adaptive and versatile cyber domain and its actors. In the cyber domain, doctrine has been slow to develop, despite the age of the Internet and ongoing disruptive cyber attacks. In 2010, the U.S. established United States Cyber Command, and almost three years later published its first doctrine for offensive and defensive cyberspace operations (Chairman of the Joint Chiefs of Staff 2013). This publication discusses the planning, integration and types of actions in cyberspace. Discussion of

actors in the cyber domain is limited. Online organizations have existed for decades and the U.S. military does not seem to have an answer to support or defend against these groups. Additional discussion, doctrine and development are necessary to enable the U.S. military planner to adequately plan for any contingency within cyberspace operations.

Recent decisions to decrease the size of the U.S. Armed Forces require the military to increase innovation to meet strategic goals. Currently, near-peer states are developing their doctrine to include full utilization of cyberspace (Chang 2014). The U.S. military must similarly develop doctrine to support Interagency and military operations through cyberspace operations in the information age. The U.S. should research and apply policies that utilize the military, political, and social aspects of cyberspace to achieve strategic goals. The combination of these factors may allow the formation of an effective cyberspace operations doctrine to meet requirements in the cyber domain.

Despite the novelty of hacktivism, the Internet, and cyber warfare, the nature of the human element in cyberspace exhibits only a scientific advancement in the evolution of warfare, not a new field of study into resistance movements. The domain has changed, yet a review of available doctrine may bridge the gap created as science marches forward and technological advancements continue to require adaptation in the military (Baumann 1997).

To combat adversary effects in this domain, the U.S. should develop doctrine with respect to cyberspace inclusive of its socio-political dynamics. Without this adaptation, the U.S ignores a greater potential to influence cultures and peoples if it focuses only on the cyber-capabilities-based disruptive, defensive, and destructive aspects of cyberspace operations. In the Information Age, every individual is armed with the ability to affect

change. An organized people can throw off oppressive regimes and governments. They only require the idea, external support, and an Internet connection.

Cyberspace operations present a deeply complicated domain, necessitating doctrine that moves beyond simple offensive and defensive maneuvers. Doctrine enables the cyberspace planner to methodically develop courses of action in support of a commander's objective. A fully armed cyberspace planner requires doctrine to guide planning efforts, establish goals, objectives and deliver effects. Without coherent planning in this regard, the U.S. remains unable to seize the initiative and dominate in the cyber domain. The U.S. must develop a cyberspace doctrine to confront the challenges of online movements and struggles.

Limitations

To avoid attribution, governments do not willingly publish information concerning their cyberspace operations. Therefore, this study is limited to unclassified, publically available information. This limitation for the discussion of this study is meant to broaden reach and distribution to the widest possible audience. Additionally, governments typically restrict or classify information concerning their cyberspace operations, naturally limiting its availability. Conversely, much has been published regarding the activities of online dissident groups and hackers.

As cyber security affects all individuals connected to the Internet, there is a seemingly limitless supply of studies and information regarding the activities of hacker organizations. Specifically, a review of the Russian use of cyber proxy forces against Estonia and Georgia provides a foundation for an expanded theory of cyberspace operations. These, and similar activities during the Hong Kong protests of 2014, are cited

in this study to analyze and develop a picture of the current state of activity in the cyber domain.

In the discussion on unconventional warfare, this research considers only those efforts to support a native resistance against its own government. Proxy wars between neighboring countries exceeds the intent of this effort.

Assumptions

The world has yet to produce a non-governmental organization that conducts so-called cyberwar to achieve its objectives. Well-known hacktivist groups such as Anonymous may aspire to the lofty ambition of cyberwar, but are more realistically limited to cyber-*battles* (Department of Homeland Security 2011). While such organizations may be employed as proxies by a state, without governmental backing, they are limited to tactical operations using common exploits and attack tools.

This study assumes that Russia supported the cyber attacks against Estonia and Georgia in order to achieve strategic objectives (Lin 2012). Russian patriotic hackers engaged targets, recruited and conducted information operations that were also in accordance with Russian objectives to pass for mere coincidence. This assumption does not conclude that all Russian patriotic hackers act under state influence, but it does assume that a few well-placed agents can provide coordination and support to an online movement.

In comparing cyber attacks and hacktivist activities during the Hong Kong protests of 2014, it is assumed that a state-sponsored or coordinated effort was not present, or not well coordinated. While such groups as Anonymous did engage government targets during the protests, these actions did not appear to reach the level of

coordination assessed during the Russian-Estonia/Georgian conflicts. This study proceeds as if the Hong Kong cyber attacks were an ad hoc effort of hacktivism without centralized planning.

Research Questions

Primary: How can cyberspace operations best be used to support online resistance movements to influence adversary national will or affect political behavior to achieve U.S. strategic objectives?

Secondary research questions:

1. What is cyber warfare, and what is its context within cyberspace operations?
2. How have cyberspace operations been conducted historically?
3. How does the U.S. Army currently conduct cyberspace operations to support conflict?

Definitions

Specific Usage of Terminology

To avoid confusion of terminology, it is important to point out the difference between cyberspace operations and other online activities. Typically, intelligence collection activities use the terms Computer Network Exploitation, Computer Network Attack and Computer Network Defense (frequently seen as CNE, CNA, and CND respectively). These terms are used only in the lexicon of older Department of Defense publications, and are not used to describe current cyberspace operations found within Joint Publication 3-12(R) (2013), nor are they doctrinally accurate for those elements subordinate to the United States Cyber Command. This study does not discuss these three

behaviors as they lie outside the bounds of published U.S. military doctrine for cyberspace operations.

Cyber Warfare

Employment of aggressive actions in the cyber domain cannot be contained in a single defintion, nor should all influential activities in cyberspace be considered aggressive. By 2013, the specter of cyber warfare had finally risen enough that the Chairman of the Joint Chiefs of Staff saw fit to produce some doctrine governing military actions in cyberspace (Chairman of the Joint Chiefs of Staff 2013). A college textbook definition of cyberwar is, "an organized attempt by a country's military to disrupt or destroy the information and communications systems of another country" (Valacich and Schneider 2012). The book *Inside Cyber Warfare* takes a somewhat more poetic approach by applying Sun Tsu-esque syntax in its definition: "cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood" (Carr 2010). Additionally, the North Atlantic Treaty Organization's (NATO) Tallinn Manual on the International Law Applicable to Cyber Warfare does not consider cybercrime as an applicable element of cyber warfare (Schmitt 2013). These disparate views of cyber warfare are myopic, and do not take into account the social power cyberspace holds to influence governments through the will of the people short of global cyberwar.

Governments might also use terms such as 'information warfare' to describe the advancement of hostilities or political goals in the cyber domain (Carr 2010). Some suggest such descriptions may be counterproductive, and that the use of the term cyber warfare does not fully circumscribe cyberspace operations inclusive of relevant shaping

and deterring operations (Williams 2014). Cyberwar is the extreme definition of cyberspace operations, expressing only the dramatic element of conflict. Regardless of the perception of war, politics, or crime, U.S. military actions in the cyber domain execute their actions under legal authorities contained within the term "cyberspace operations." This document employs the term cyberspace operations to include cyberwar and cyber warfare, describing governments' support of online organizations and hacktivist activities, as well as disruptive actions against information systems.

Cyberspace Operations

Cyberspace operations include those actions as defined within Joint Publication 3-12(R) *Cyberspace Operations* (2013): Offensive Cyberspace Operations, Defensive Cyberspace Operations, and Department of Defense Information Network Operations. Cyberspace operations support all levels of war Strategic, Operational, and Tactical (Chairman of the Joint Chiefs of Staff 2013).

Hacktivism

Hacktivism is the evolution of civil disobedience to incorporate information system exploitation, or hacking, in support of a political or social cause (Baase 2008). Hacktivists use technical skills to hack information systems in support of their efforts. These effects are typically disruptive (politically, socially, or economically) to their intended targets. The exploitative actions and behaviors of hacktivists are the objective of this research, as well as how hacktivists might be supported to achieve foreign policy objectives.

Hacktivists typically reside in a neutral area in regard to support by states. Once hacktivist groups receive external support, or seek to attack and overthrow a government, then it may be more appropriate to call them cyber militias or cyber guerillas (Ottis 2011; see also Applegate 2011). Regardless of the status of the hacktivist, this study considers technically savvy, politically-motivated hackers as hacktivists.

Unconventional Warfare

Unconventional Warfare is the method by which the U.S. supports an insurgency. The broad definition of unconventional warfare from Joint Publication 3-05, *Special Operations* (2014), possibly allows for the inclusion of hacktivists and online organizations for the disruption or overthrow of a government, potentially filling the role of a guerilla force (Chairman of the Joint Chiefs of Staff 2014). To ensure a clear understanding of how unconventional warfare applies to this research, the following quotation constitutes the definition of unconventional warfare:

> *Unconventional warfare* is defined as activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and a guerrilla force in a denied area. (Chairman of the Joint Chiefs of Staff 2014)

Authority to conduct unconventional warfare resides in Section 167(j), Title 10, United States Code. Currently, the only organization authorized to conduct unconventional warfare, in cyberspace or otherwise, is United States Special Operations Command.

Significance

This document explores how cyberspace operations can best be used to support online resistance movements to influence adversary national will or affect political

behavior to achieve U.S. strategic objectives. This gap between how the U.S. conducts cyberspace operations and hacktivists with shared goals is an exploitable seam that appears untouched. The U.S. trails behind other nations in their efforts to influence and mobilize hacktivists to achieve foreign policy objectives through cyberspace and must consider how to adapt current doctrine to support online insurgent groups, or to counter them.

This study is the first to consider the application of cyberspace operations and interaction with online hacktivist organizations in order to bridge an apparent gap in doctrine. Future challenges in the cyber domain continue to develop in a connected world where political movements are empowered by the Internet, social media, and the rapid flow of information. U.S. leadership must understand current limitations of doctrine to meet this future challenge, and develop the necessary solutions and doctrine in a new domain of conflict.

CHAPTER 2

LITERATURE REVIEW

A study of hacktivism, cyberspace operations, and unconventional warfare encompasses the missing area of defined policy on how the U.S. engages, supports or influences online dissidents. This research explores the characteristics of each of these areas to identify related elements and determine how best to construct a model suitable for U.S. military and Interagency operations to counter adversarial nations with anti-government hacktivist activities. Countries swiftly adapt to operations in the cyber domain in order to fully exploit its potential. The U.S. must not lag behind in its research and study of warfare in this new domain.

To establish a shared understanding of how best to employ cyberspace operations to impact organizations, it is necessary to review current and historical developments of both doctrine and political activism. A review of the history of political activism and hacktivism, its roots and origins, as well as hacktivism's current practice in the political arena describes the current cyberspace operating environment and how it affects governments. A brief discussion on the use of cyberspace operations by the U.S. military is also included to provide some understanding of the types of operations conducted, and the current disposition of U.S. cyber doctrine. Also included is a simple and brief review of unconventional warfare with its phased model of support to insurgencies in order to establish the foundational understanding necessary to visualize how cyberspace operational support to online organizations has relevance to unconventional warfare.

Political Activism

Political activism represents the ways and means in which citizens act to achieve a desired political end state. Political activism can include actions as simple as discussing political concerns with a neighbor, or influencing a prominent civil or government figure through conversation It can also include large gatherings to show support and use print media to transmit an organization's desires to a broader audience. Political activism may also include strikes, petitions and protests, both peaceful and violent; the latter are included under civil disobedience as a means to achieve political objectives (Norris 2005).

Political activism evolved to include civil disobedience as active resistance in efforts to remove undesirable political bodies (Department of the Army 2011). Examples of civil disobedience include protests against the International Monetary Fund in Seattle and the World Bank in Washington D.C. (Gill 2000). Protestors chained themselves to each other, fought against riot police, and used other tactics in efforts to affect change. An active resistance incorporates as many different methods available to undermine the political influence and power of the targeted regime. While not always violent, political activism continues to discover new ways to influence governments. The extreme use of political activism may result in an insurrection to remove a governing body from power and establish a new political regime.

Political activism continues to evolve today to include use of the Internet as a means to transmit information concerning a cause. The Internet has provided the world with the ability to rapidly identify individuals of like political persuasion through social networking sites, email, blogs, forums, and other websites. Hacker activists have

continued civil disobedience into the cyber domain as they seek to disrupt political processes, government services, and information in their favor. This study supports and expands military research of resistance organizations and insurrections into the cyber domain.

History of Hacktivism

From Personas to Hacktivists

Nearly every country in the world hosts private users of the Internet. Using the Internet, individuals generate online personas to pursue interests, find entertainment, engage in commerce, and seek information as they interact in the cyber domain (see figure 1). Online personas can lead to underground or nefarious groups that promote a political agenda either through the distribution of information, or through activities called hacking. The latter of these groups are often called hacktivists.

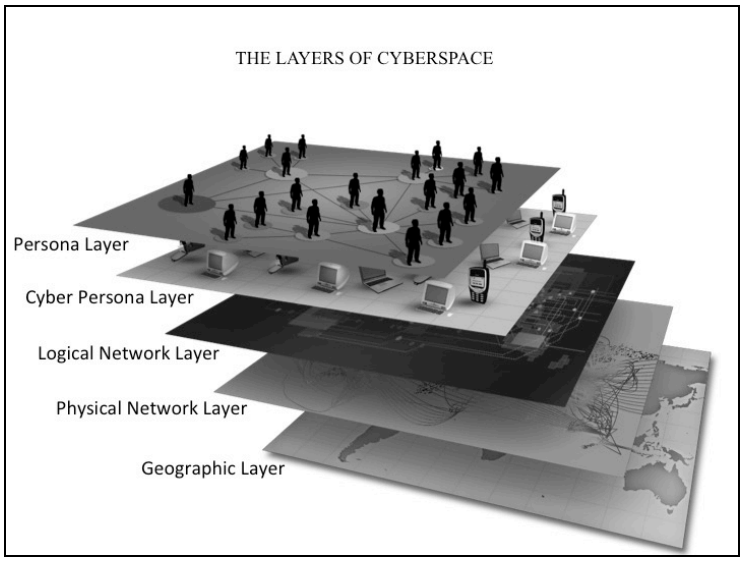


Figure 1. The Layers of Cyberspace

Source: Chairman of the Joint Chiefs of Staff, *The Layers of Cyberspace* (Washington, DC: Department of Defense, 2013), I-3. The hacktivist exists at the Persona Layer and operates in the Cyber Persona Layer. This layer consists of email accounts, phone numbers, social networking accounts, handles, aliases, etc. It is at this layer where hacktivists coordinate for effects on the Logical Network Layer.

Development of the Internet provided hacktivists a means to perform deeds comparative to conventional civil disobedience. Hacktivism, political hacking or hacker activism, has existed since the mid 1980s. As early as 1994, the peculiarly named Critical Art Ensemble, and a different group later in 1998, the Electronic Disturbance Theater, saw the Internet as a means of resistance to influence politics (Taylor and Jordan 2004). Ultimately, in the mid-1990s, the term "hacktivist" was coined by a member of the Cult of the Dead Cow, another group of hackers seeking their own political objectives (Mills 2012). Some of their initial efforts largely revolved around attempts to deny network nodes and websites they believed were opposed the Zapatista uprising in Mexico (Taylor and Jordan 2004).

These organizations can have a tremendous impact on societies and culture, whether for good or bad. Organizations like WikiLeaks are held in both high and low esteem by people and governments across the planet (Hansen 2010). To paraphrase a popular adage, "One man's [hacktivist], is another man's freedom fighter." The alternative view was best articulated by President Ronald Reagan when he declared, "terrorists [or hacktivists] are always the enemy of democracy" (Reagan 1986). Despite President Reagan's view, it seems that hacktivists only represent an enemy to individual freedoms when used to disrupt the free flow of information to a nation's citizens, a key indicator of individual freedoms. How a hacktivist organization can be utilized as a "freedom fighter" and not an enemy of individual freedoms requires further discussion.

Russian Exploitation of Hacktivism

Recent examples that may display the hacktivist as a "freedom fighter" include the actions, and effects, of alleged Russian cyberspace operations during the Estonian and Georgian conflicts in 2007-2008. These events, and others, represent potential benefits to governments working with hacktivists. They also present ideas relevant to modern unconventional warfare in the cyber domain.

The actions and reactions of Russia and Estonia demonstrate a change in how conflict could be executed in pursuit of political objectives. Russia discovered the potential benefit of hacktivism when its nationalism was insulted while the government of Estonia relocated Soviet monuments in 2007. The Russian reaction included a three-phased cyberspace attack against Estonian information systems perpetrated by patriotic hackers (KGS NightWatch 2011). As a result, Estonia has been a lead proponent in

defining cyber warfare for NATO, aspiring to limit its effects and spare other nations from being victims (Schmitt 2013).

These events demonstrate potential effects from cyberspace operations for states in pursuit of political objectives. Additionally, these effects can be achieved outside of conventional conflict as states avoid attribution from offensive cyberspace operations. Russian hacktivists, perhaps with support from the government of Russia, quickly attacked and defaced Estonian government websites in the initial phase of operations against the Estonian government followed later by attacks with even greater disruptive effects (Ottis 2011).

Russian actions represent a shift in how global politics can influence governments. Political activism, through the Internet, is now able to transcend borders to achieve an effect that would have historically required thousands of individuals risking personal harm and injury, conventional military intervention, or at least publically declared political and economic sanctions.

In the space of a few short years, Russia's conflicts demonstrated the value of a civilian hacktivist element in cyberspace operations by disrupting politics and further causing chaos to achieve strategic objectives (Bumgarner and Borg 2009). Although hacking has been around for decades, it was the cyberspace attacks against Estonia in 2007 that first introduced the world to possible state-sponsored unconventional warfare through cyberspace (Ashmore 2009). Building upon the successful employment of hacktivism against Estonia, Russia continued to support patriotic hackers, or Russian cyber militias and cyber guerillas, in its campaigns against Georgia, Lithuania and later against Kazakhstan (U.S. Cyber Consequences Unit 2009). Exploiting the favorable

conditions of a weak government during the Russian-Georgian war of 2008, hackers overwhelmed the Georgian public and private information infrastructure (Basilaia 2012).

Russian Military Synchronization with Cyberspace Operations

While Estonia's cyberspace attack evolved from the removal and replacement of a bronze statue and stayed within the cyber domain, the Georgian event coincided with military action. The Georgian cyberspace attack even appeared coordinated with military operations, lending credibility to the possibility of communication between the cyber militias and the government (Bumgarner and Borg 2008). For the first time in history, cyber militias–hacktivists–and conventional forces operated under the same command and control structure to achieve an operational objective.

Russian cyberspace operations in Georgia were a supporting effort, affecting similar psychological and economic impacts as the Estonian campaign. Once set in motion, the attacks were initially focused and successful; however, unpredictability set in and the cyber attacks appeared more chaotic, and not always executed with military precision. As a group, hackers often swarm around a tool and its target when that target becomes popular. While the initial attacks may have been coordinated, later attacks were the result of trendiness, and sporadically continued after Russia's planned timeline ended (Ottis 2011).

The nascent cybersecurity capabilities of Georgia in 2008 were no match for coordinated Russian cyberspace operations. Russian online recruitment of patriotic hackers quickly mobilized a cyber guerilla force disrupting Georgian infrastructure. Organic Georgian infrastructure, unable to meet the bandwidth demands of the

distributed denial of service attack, ultimately moved government and financial website hosting to Estonian servers (Basilaia 2012). The National Bank of Georgia also ceased operations for 10 days due to the attacks (AFCEA International 2012). The effect was a diminished Georgian government unable to defend against both conventional and digital attacks.

The economic and psychological impact on the victim country again proved valuable to Russia's military and political objectives. The economic interruption of web-based commerce, and the seemingly scant media coverage of the cyberspace attacks, enabled Russia to benefit from the attack without fear of international response (Bumgarner and Borg 2008). There were few to no reprisals from the United Nations and other bodies because Russian civilians, or patriotic hacktivists seemingly conducted the great majority of attacks. This enabled the Russian government to avoid taking direct credit, or blame, for the disruptive attacks.

Russian cyberspace operations were able to demonstrate the viability of using hacktivists as a method to achieve strategic objectives. Advancing the definition of combined arms maneuver, the events in Estonia and Georgia demonstrate the possibility to militarize online organizations as a viable combat method, providing support to conventional forces, and affecting political maneuvering. It is the lessons learned and the model developed through Russian actions that hint at the possibility of using cyberspace as a discreet effort to influence online dissident organizations and hacktivists.

Influence of Social Media

Social media provides the opportunity for hacktivists to promote their cause and campaign in social spheres. In particular, the ubiquitous hashtag (#) prevalent in popular

social media venues such as Facebook, Twitter, and foreign equivalents, enables hacktivists to advertise their activities, gain support and disseminate tactical victories (Koyfman 2014). Recent Russian operations in Ukraine coincided with the development of pro-Russian factions prompting their hashtag #OpRussia. A counter faction promoted their cause with #OpUkraine. Both sides hacked each other's websites, forums, and government sites throughout the recent events in Ukraine in order to disrupt the other side's ability to wage conflict, while Russian rebels conventionally engaged Ukrainian forces.

As a result of its effectiveness, social media is a target for disruptions by governments, or exploitation by hacktivists, both of which induce cultural responses. Attacks that disrupt social media produce a swift response, and can garner support for a cause almost immediately. Conversely, using social media as a means of producing propaganda causes a vitriolic response as well (Rantapelkonen 2013). Social media as a means to foment rebellion or civil disobedience proved an effective method; a government response that shuts down social media services is likely to fall immediately into disfavor by its populace (Rantapelkonen 2013).

Social media has demonstrated its effectiveness to rally popular support for a cause. Recent uprisings in the Middle East in 2011 caused governments to block social media sites in efforts to contain citizen engagement (Ghannam 2011). China is also known to censor social media when issues that embarrass or undermine governance become too popular (Bamman, O'Connor and Smith 2012). Other nations also fend off popular uprisings through deterring or disrupting social media outlets. Social media, as an

extension of the people, continues to show its power to envigorate latent movements into national events.

The application of social media to garner support for, or against, a cause continues to expand as mobile devices and media sharing applications grow to reach global audiences. As governments already employ the Internet's social connectivity to manage their populations, Russia's military application of the social aspects demonstrates a potential trend of exploitation. It is important for the military planner to consider the application and influence of social media relevant to operations.

Activities and Effects

Nearly every characteristic of the Internet is asymmetric when used offensively. During the Estonian and Georgian cyberspace attacks, using hacktivist non-state actors, information and capabilities were published to hacker forums and resulted in a significant threat to the cybersecurity of these two countries. Hacker organizations on the smallest of budgets can achieve enormous effects, even when aspiring hackers are poorly trained (Ottis 2011). Scholars of cyberspace operations posit how state-produced cyber capabilities might be used to deter an adversary. The Russians effectively demonstrated this theory while abusing their neighbors and limiting costs from conventional operations (Clarke 2010).

Recent research into volunteer hackers, or hacker militias, indicates that recruiting from the populace through social media is a viable option (Basilaia 2012). Volunteer cyber militias, or hacktivists, conducting cyberspace operations are population-centric; they represent the cause of the people, whether offensive or defensive, depending on ones point of view. Specifically, when using cyberspace operations to achieve strategic goals,

Russia understood how cyber power might be used to "coerce, disrupt, or overthrow a government or occupying power by operating through or with [cyber militias and hacktivists]" (Department of the Army 2011).

The history of hacktivism shows a flow of Internet power from an elite, technologically capable few, to the masses. Hacktivists come in every degree of capability. Some merely support a cause through transmission of a hashtag, while others endeavor to employ capabilities to disrupt Internet activity. More advanced applications involve the manipulation of social networks by nations to influence and attack an opponent. Russian actions demonstrated a model presenting the possibility to conduct warfare in a new domain outside of the apocalyptic cyber war view held by many.

The evolution of political activism to include combined arms maneuver with hacktivists demonstrates massive potential to influence populations and governments. Russia's actions against its neighbors enlisted the support of cyber militias to execute disruptive attacks against a target nation. The possibility exists that future operations may not include a conventional force to achieve initial objectives to set the conditions for a strategic victory, but rather cyberspace operations executed covertly with hacktivists to achieve the desired end state.

How the US Army Conducts Cyberspace Operations

US military joint doctrine does not prescribe an implementation policy for cyberspace operations, but rather defines the activities within the cyber domain in the broad category of cyberspace operations. The implementation is left to the design and intent of a Commander and his staff (Chairman of the Joint Chiefs of Staff 2013). Typically, offensive actions are couched under the terms: Offensive Cyberspace

Operations, and Cyberspace Attack (and, arguably, Defensive Cyberspace Operations–Response Actions). Within these definitions, actions in support of hacktivists to influence an adversarial government must be inferred, as it is not explicitly stated. This represents a gap in cyberspace operations doctrine.

Due to the classified nature of U.S. cyberspace operations, validated information on US cyberspace operations is limited. However, members of President Obama's Administration admitted in 2012 that the U.S. was responsible for the Stuxnet attack against Iran (Nakashima and Warrick 2012). Stuxnet was a piece of malware that caused significant damage to Iranian nuclear capability. Despite the alleged disclosure, the event does not fully describe how the US actually conducts cyberspace operations.

Stuxnet was developed and released prior to the establishment of the United States Cyber Command in 2010. U.S. Cyber Command holds responsibility for Title 10 actions in cyberspace. As the command did not exist prior to 2010, it would seem unlikely it participated in the planning and execution of the operation. Therefore, with available unclassified information, it is still unclear as to how the U.S. military conducts cyberspace operations.

Even the recent security breaches at the National Security Agency by Edward Snowden exposed only intelligence collection activities, and not means and methods of cyberspace operations under Title 10 and Joint Publication 3-12(R) *Cyberspace Operations*. The public is currently confined to speculation and published doctrine on how cyberspace operations are conducted.

During the course of developing this study, the Department of Defense released an unclassified document entitled *The DOD Cyber Strategy* (Secretary of Defense 2015).

This document outlines five strategic goals for cyberspace operations. The goals center on the philosophy of build, defend, defend some more, shape and deter, and build alliances. An observant reader must interpret this published policy to understand that shape and deter indicate a more offensive nature of cyberspace operations. The true nature of deterrence that this strategy describes remains classified. Limiting the U.S. to defensive actions implies that it will be the first to encounter offensive cyber capabilities built by competitors. In the offense, a cyberspace attack only has to be right once, whereas the defender must correctly defend each time (Poulsen 2015). A predominantly defensive strategy does not seem plausible.

Current U.S. doctrine is therefore limited in explaining the application of cyberspace operations to support a strategic end state, and how to interpret such activities from a political and military point of view. It is unlikely to expect a well-defined policy any time soon from the Joint Staff or the White House (Parker 2014). Recent hacks against Sony Entertainment elicited a response from President Barak H. Obama wherein he termed the attacks 'cybervandalism' and not an act of war (Bradner 2014). Statements and disclosures like these further cloud the understanding of how the US conducts Title 10 cyberspace operations and how it interprets similar attack behaviors globally.

Conversely, it is this same complexity of the Internet and cyber attacks that demonstrate the potential application of alternative cyberspace operations as a new means with which the US can influence its adversaries. Perhaps this ambiguity may have been foreseen, as developers did not write limitations and specific applications of cyberspace operations into doctrine. Regardless, cyberspace planners must consider how best to proceed under ambiguous guidance and shortcomings in doctrine.

There is a gap in doctrine that limits the ability of the U.S. military to conduct operations in a manner that exploits all characteristics of the cyber domain, therefore consideration of these characteristics of the Internet and its players should be included in future development of doctrine. Specifically, these gaps are the consideration of hacktivists as cyber militias, or cyber guerillas for inclusion in cyberspace operations against a target.

Although current doctrine does not explicitly state the manner in which hacktivists might be used to further strategic policy, U.S. doctrine does contain significant guidance on the conduct of unconventional warfare and the use of dissident organizations. Unconventional warfare doctrine already includes an adaptation for Civil Affairs to support the seven phases of unconventional warfare. Civil Affairs has other roles beyond unconventional warfare however, and there is currently doctrine providing instruction on its support to unconventional warfare. Cyberspace operations doctrine however, does not currently have this adaptation.

Unconventional Warfare

Following World War II, President John F. Kennedy promoted the efforts of unconventional warfare as a way of achieving national strategy (Department of the Army 2011, 1-1). The U.S. understood that small wars require special attention, strategy and support beyond its conventional cousin. The U.S. military and the Interagency historically used organizations within denied areas to promote U.S. national interests. Foreign countries conducting counterinsurgency operations often experience reduced capability to effectively manage external conflicts, and must divert national resources internally in order to maintain stability. These conditions produce an environment that

enables the U.S. to pursue its global and regional objectives with reduced interference from adversarial nations seeking to undermine individual freedoms.

There are several dynamics of successful insurgencies that enable popular discontent to develop into an effective and organized movement. Fundamentally, unconventional warfare seeks to exploit three conditions to achieve US objectives: a weak government, a segmented population, and favorable terrain to develop a resistance (Department of the Army 2011). Along with these conditions, there are the dynamics of a successful insurgency, such as organization, ideology and leadership. These dynamics are only lightly touched upon in this study and are recommended as future research topics. As cyberspace operations doctrine requires an adaptation for unconventional warfare, so must all the tenets of unconventional warfare receive the necessary research to develop the appropriate model for adaptation. This study limits the discussion to the seven phases of unconventional warfare, and leaves the relevant dynamics of the cyber domain for future research and integration into U.S. doctrine. For a complete review of these fundamentals see Chapter 2, "Special Forces Unconventional Warfare" (2011). Recent research demonstrates the impact of modern technologies on insurgencies and the informed reader should also consider those discussions relevant to the dynamics of unconventional warfare (Metz 2012).

In order to assist in planning unconventional warfare, the U.S. has established a doctrinal framework consisting of seven phases. Special Forces, Civil Affairs, and Military Information Support Operations support these phases. Additionally, the fundamentally political nature of unconventional warfare requires planning and involvement with joint and Interagency support. The following sections of this chapter

condense and summarize the seven phases of unconventional warfare; for a thorough study of the topic the reader should engage Training Circular 18-01 *Special Forces Unconventional Warfare* (2011).

Phase I–Preparation

Preparation typically includes a study and assessment of the target area drawing upon available intelligence. During this phase, in conjunction with Military Information Support Team experts, the U.S. conducts an assessment of those organizations that possess the capability to support the populace's anti-government movement. The assessment provides information on identified resistance groups to include their strengths, weaknesses, relationships, logistics, tensions, objectives, and capabilities (Department of the Army 2011).

Previous doctrinal publications outlined planning factors for the success of an insurgency required that "the insurgents must have a program that explains what is wrong with society and justifies its actions" (Headquarters, Department of the Army 2003). Current doctrine provides the same point in discussing the dynamics of successful insurgencies in that they contain properly defined objectives relevant to Ideology (Department of the Army 2011). Unconventional warfare needs to be synchronized with the public's desire for improvements and basic freedoms. An example of this might be the free flow of information as a critical requirement for a unifying ideal.

U.S. shaping operations establish the conditions for successful U.S. involvement in unconventional warfare. The length of time to conduct Phase I Preparation is indeterminate. Only through continual assessment and observation does an understanding of the environment occur, and supports timing of phase transitions. Assessing and

shaping allows the U.S. to determine proper support to a cause, and its leadership, enabling an opportunity to progress to the next phase.

Phase II–Initial Contact

Traditional unconventional warfare requires considerable planning for initial contact with Irregular Forces. The right guerillas and their leaders, with relevant and specific skills, must be vetted and assessed. Initial contact and infiltration, as described in unconventional warfare doctrine, includes contacting resistance leadership or a government-in-exile to determine if the cause is compatible with U.S. strategic ends. This contact enables the assessment of whether the organization is willing to accept U.S. assistance.

The initial contact may even include the infiltration of a Special Forces pilot team, or potentially the exfiltration of a resistance leader to aid in the assessment and planning of the unconventional warfare campaign. These interactions enable further area assessment and assist in determining the level of support necessary for successful accomplishment of unconventional warfare (Department of the Army 2011, 3-3).

Phase III–Infiltration

Typically, a Special Forces team infiltrates the joint special operations area, establishes communications with its base of operations, and then contacts the resistance organization to begin integration (Department of the Army 2011). As necessary and applicable, this initial team coordinates for the future infiltration of follow-on teams into the area of operations. These teams integrate with, and conduct an assessment of,

resistance counterparts and their effectiveness in the unconventional warfare campaign throughout the operations area.

The infiltration of teams is a decisive point in supporting an unconventional warfare campaign. A successful infiltration enables assistance to the resistance in the form of planning, organization, and command and control. Additionally, an infiltration enables the precursor assessment for continued support by the U.S. government. In conditions where the infiltration of Special Forces teams is less desirable (i.e. limited war), planners should consider the exfiltration of resistance leadership for the training and organization of a resistance (Department of the Army 2011).

Successful infiltration lays the groundwork for greater efficiencies in a resistance organization. Once Special Forces teams have linked with partners, progress for increasing the capacity of the resistance can proceed at a faster pace. Special Forces teams assist the resistance cadre with developing, planning and coordinating for future operations.

Phase IV–Organization

Organization begins once advisors have been able to integrate and communicate with resistance leaders. Development of an organization under unconventional warfare doctrine requires rapport building and ensuring that the resistance and the U.S. share similar goals and objectives. The resistance organization must prepare itself for logistical sustainment once it begins combat operations in later phases by establishing a resilient infrastructure through planning and coordination with advisors (Department of the Army 2011).

The organization phase considers all future planning and activities of the resistance. The insurgents and advisors plan and consider future operations, security, acceptable U.S. levels of influence, and the extent of cooperation between the two. It is during this phase that advisors also assess and determine the strengths and weaknesses of the resistance to determine appropriate levels of assistance or aid.

All resistance organizations are unique to their circumstances. It is critical for advisors and planners to understand the organizational structures and capabilities. The organization of the resistance also determines how an auxiliary is structured (Department of the Army 2011). The auxiliary is a portion of the population that provides "active clandestine support" to a guerilla force (Department of the Army 2011). A clear view and understanding of a resistance and all its functions, enablers, and support facilitate planners in developing a concept for expanded operations beyond the resistance's initial capacity.

Phase V–Buildup

During buildup, the intent is to expand nearly every aspect of the insurgency preparatory to employment. Doctrinally, U.S. advisors increase support through intelligence, counterintelligence, and indications and warnings to the resistance group. The intent is to enable confidence targets to build the capacity of the resistance. The U.S. provides the analytical background to the resistance as they seek to identify those objectives that, once accomplished, will further their goals.

During this phase, the intent is to expand nearly every aspect of the insurgency, and its warfighting functions, preparatory to full combat employment (Department of the Army 2011). All resistance capacities, from tactical to logistical, increase to support

future operations during Phase VI, Combat Employment. Tactical objectives are the immediate aims of insurgency actions during the buildup phase. Initial tactical gains seize the initiative in support of operational goals.

Constant and continuing assessments by the planning team, theater Military Information Support Teams, Civil Affairs, and the intelligence community help drive the targeting process by identifying suitable engagement areas for insurgents during the buildup phase based upon capability and capacity (Department of the Army 2011). This support increases the opportunities for success as the resistance secures its infrastructure and organization transitioning into combat employment.

Phase VI–Combat Employment

Employment of the resistance force is the execution of expansion and buildup plans developed during Phase V. The purpose is the attainment of political objectives. Much of what occurs during employment is not exclusive to an insurgency, but includes disrupting communication nodes, exposing key leaders and disrupting targets in the government's rear area (Department of the Army 2011). Insurgent activities also require Military Information Support Operations to exploit tactical gains; an attack without advertisement does not promote or assist the resistance in its popular and political objectives. Planning combat employment ensures the layering of effects paired to the capabilities of the insurgency.

Consideration for Phasing and Timing and the employment of guerilla operations determines the tempo and scale of attacks. The three phases, Latent, Guerilla, and War of Movement comprise the Phasing and Timing contstruct for the progression of unconventional warfare (Department of the Army 2011) The Latent phase typically

precedes the other phases, as an insurgency generates support, and does not include a defined strategic end state. General War and Limited War have specific end state objectives for tactical engagements. Planning determines the end states and conclusion for combat operations prior to demobilization. An insurgency does not require a complete transition to all insurgent Phasing and Timing elements, and can be successful without all three (Department of the Army 2011).

Combat employment concludes when objectives are met. The timeline of insurgencies do not prescribe the time necessary to achieve its goals. Planners must consider, and assess, the progress of the insurgency to effectively aid in the decision to transition to the next phase of an insurgency and avoid diminishing the success of the insurgency.

Phase VII–Transition

The transition from an insurgency once objectives are obtained requires an adjustment from disruptive operations to supporting the newly established order (Department of the Army 2011). A danger also exists that insurgents may return to other disputes or criminal behavior. How demobilization, transition, and rehabilitation occur affects the post-conflict attitudes of the people and the government towards the U.S.

Unconventional warfare doctrine describes some of these rehabilitating activities as using members of the resistance as "local militias" and making efforts to prevent them from starting or engaging in new political conflicts. During the transition, and to aid rehabilitation, Civil Affairs and Military Information Support elements are important in ensuring that post-conflict circumstances meet the expectations of the resistance organization (Department of the Army 2011). Civil Affairs has a prescribed role of

support for each phase of unconventional warfare, and plans for its role accordingly. Using the resistance to support the new government represents a proactive measure towards a positive and successful transition.

Additional Considerations

The phases of unconventional warfare require proper coordination and planning to ensure the gains and successes of the insurgency continue after the completion of each phase. Unconventional warfare requires a significant planning effort to coordinate and execute, as well as to understand measures of effectiveness that signal planners to transition from one phase to the next, and assess the progress of the resistance movement. Paramount to all these operations is the information and logistical support to both Special Forces advisors and the resistance to achieve strategic objectives (Chairman of the Joint Chiefs of Staff 2014).

Not every insurgency completely and clearly implements each phase as described (Department of the Army 2011). Each resistance is unique in its popular support, geography, cause, and objectives. The fundamentals of support to an insurgency are necessary regardless of the operational environment; doctrine is the guide to campaign success. The unconventional warfare planner must continually assess the status of the resistance to understand when and how to transition from each phase (Department of the Army 2011). Without this understanding, popular causes rise and fall without the necessary guidance and support to achieve their desired end state.

It is important to understand that unconventional warfare can be applied to disrupt the external efforts of national power from the targeted nation. As a nation attempts to fend off an insurgency, it can experience limited ability to externally focus its efforts

internationally in pursuit of its objectives. For this reason, unconventional warfare is a relevant capability for the U.S. to employ to disrupt adversarial governments that engage in belligerent regional activities against their neighbors. As the country focuses inward, it consumes capacity meant for external military, diplomatic, informational and economic endeavors.

Conclusions

A review of the characteristics and evolution of political activism into the cyber domain presents new opportunities for conflict and countering political oppression. Hacktivists display characteristics suitable for use as a cyber militia or auxiliary in support of an insurgency and demonstrate the potential for future use in conflicts. Russia demonstrated their ability to exploit the cyber domain through the use of hacktivists in a manner consistent with principles of unconventional warfare. The U.S. has a gap in doctrine because it does not synchronize cyberspace operations and its applicability to online groups, organizations and hacktivists. Unconventional warfare has established doctrine for the planning and development of campaigns to assist resistance organizations to achieve desired change. This gap in doctrine between unconventional warfare and cyberspace operations relative to online resistance groups requires development, and consideration, in how the military and Interagency fully engage actors in the cyber domain. The players are already in the cyber domain and the U.S. is without a construct for engagement.

Unconventional warfare doctrine describes the characteristics necessary for a successful insurgency. Aspects of adaptability, targeting, rear-area attacks, information support operations, support of the populace, and infrastructure requirements for an

insurgency have striking similarities to hacktivist activities and requirements. Hacktivism represents a possible new venue for engaging in a limited war insurgent campaign, with minimal casualties and disruptive effects on the population. While general war may not be possible with cyberspace operations, not all phases of unconventional warfare are necessary to achieve political and military goals (Department of the Army 2011). The following chapters discuss a potential adaptation of unconventional warfare doctrine and how it might be applied to cyberspace operations and support to an insurgency through online organizations and hacktivists.

CHAPTER 3

RESEARCH METHODOLOGY

This study began with the problem of how to best engage online resistance organizations in support of U.S. policy. It reviewed current definitions relevant to the problem including cyberspace operations doctrine, and publications related to resistance groups. The literature review highlighted a gap in how the U.S. conducts cyberspace operations to support resistance organizations in the cyber domain.

This study considers the major aspects of online interaction and hacktivism to develop a model suitable for employing Internet-based groups in support of U.S. objectives.[1] Hacktivists, operating like guerilla forces, have been employed by Russia as a supporting effort to achieve objectives in the Russian sphere of influence. In hacktivism, social dynamics also play a critical role, and hacktivist operations do not focus solely on technical capabilities for success. A cause must also attract and motivate others, an effort critical to achieving the desired strategic objectives in cyberspace. Hacktivism struggles to effectively change governments because it is an ad hoc effort in anti-government operations. The seven phases of unconventional warfare, discussed in Chapter 2, present a campaign guide to insurgencies through which a model is developed relevant to the cyber domain.

Cyberspace offers a potential opportunity to implement unconventional warfare within a new domain using hacktivists, or cyber guerillas, as a proxy force. Online

[1] This study seeks to identify a model to plan for unconventional warfare solely in the cyber domain, as opposed to using cyberspace operations as only an occasional supporting effort to a resistance as discussed in other research endeavors. See Eidman and Green, 2014

resistance organizations invoke consideration and parallels towards unconventional warfare in this new domain. Hacktivists have proven that through the Internet, these entities can organize to resist governments and corporations. The missing dimension revolves around how these organizations might better, and successfully, resist governments to achieve their desired change. Russia has already demonstrated opportunities to undermine foreign countries in Eastern Europe with weakened governments and insufficient cybersecurity capability that leaves them vulnerable to organized hacktivists.

Methodology and Model

The proposed model for solving how best to conduct cyberspace operations in support of online dissident organizations to achieve U.S. strategic goals is an adaptation from the Seven Phases of unconventional warfare. Each phase of unconventional warfare contains fundamental principles of support to an insurgency that may extend into the cyber domain and cyber militias. This model is comprised of six phases directly derived from the principal U.S. unconventional warfare doctrine.

This study postulates that a review and update to Army, Interagency, and joint doctrine regarding unconventional warfare and its application in cyberspace may provide a new opportunity in the cyber domain to counter adversarial governments. To do so, the research analyzed several relevant topics and characteristics of unconventional warfare, hacktivism, and online culture to span the gap between theory and doctrine. Fundamental to this theory is the desire for change and motivation common in political activism.

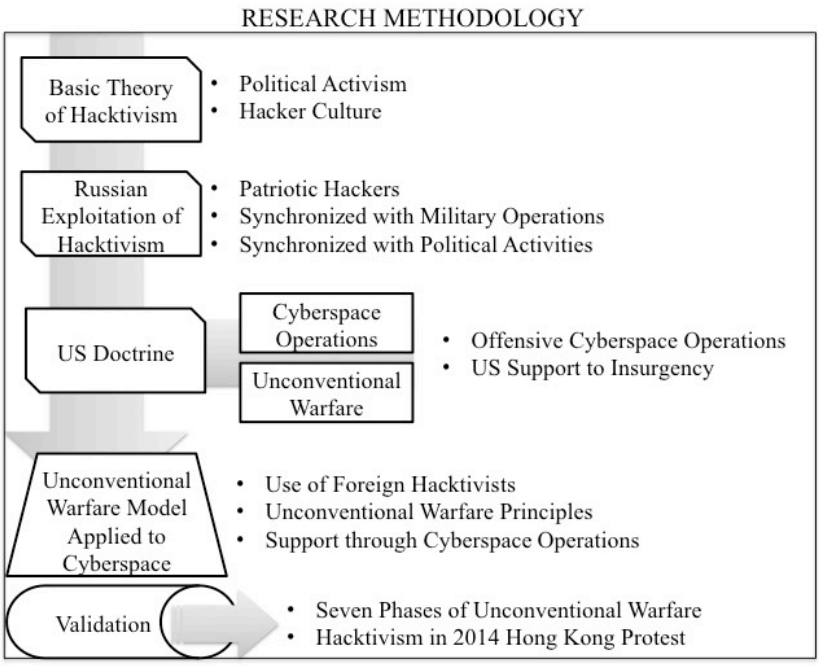


Figure 2. Research Methodology

Source: Created by author. Current U.S. unconventional warfare doctrine forms the foundation for a proposed cyberspace unconventional warfare doctrine. The model is validated using the 2014 Hong Kong Protests.

To support a resistance, Russia provides the most recent, successful example of how a nation might utilize hacktivism to achieve its national objectives. Russia coordinated and synchronized hacktivists with conventional military operations against Georgia, demonstrating the potential for viable, simultaneous command and control of hacktivists alongside combined arms maneuver.

The inherent activities of hacktivists foster a cyberspace insurgency environment. Required is a model and doctrine for the US to exploit this opportunity through expanded employment of cyberspace operations. Such a model does not currently exist within the doctrinal libraries of the US military. This likely limits U.S. ability to fully exploit the

full offensive power of the internet in achieving strategic goals without “boots on the ground”, massive military expenditures, or overwhelming fear of attribution.

Analysis

Validation of the new six-phased model for cyberspace operations within an unconventional warfare construct necessitates a comparison of real-world hacktivist activities. The validity of the model is evaluated using hacktivist and government activities during the Hong Kong protests of late 2014. While this was not a successful endeavor like the Russian engagements in the first decade of this century, the Hong Kong protests provide information for an initial assessment into the plausibility of the model.

The proposed solution to the gap in U.S. cyber warfare doctrine is to adapt the current doctrinal model used in unconventional warfare. The new model consists of six phases generally following its principal doctrine with definitions expanded to include planning considerations relevant to the organization and motivation of hacktivists

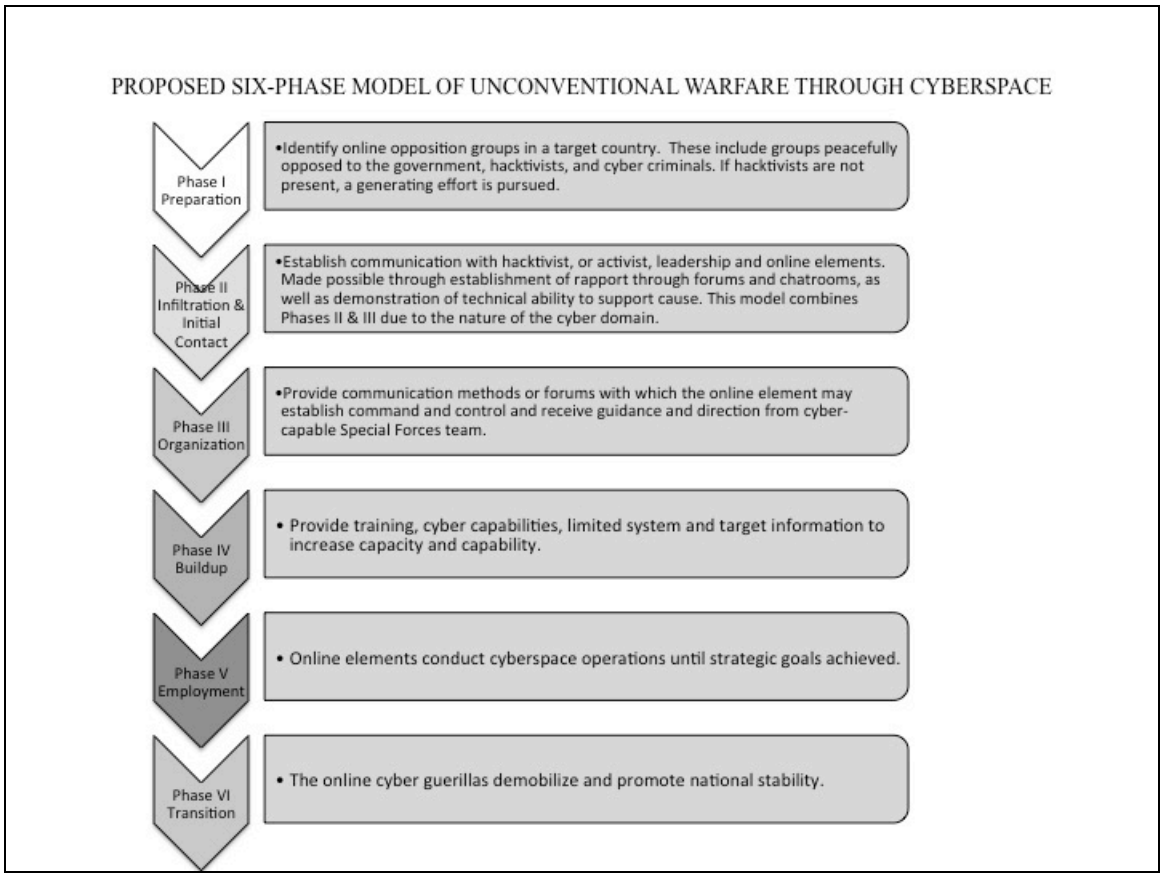


Figure 3. Model for Planning Unconventional Warfare in Cyberspace

Source: Created by author. This model is a direct adaptation of the seven phase Unconventional Warfare model found in U.S. doctrine. It combines initial contact and infiltration, and provides a brief definition of activities during each phase relevant to the cyber domain.

CHAPTER 4

ANALYSIS

Background

Social and political struggles of the information age now use the cyber domain to promote ideology and affect change. This utilization benefits individual citizens, as well as governments, as an extension to elements of national power and strategic goals. Since 1984, the Internet has provided a means to advance almost any ideology through either information promulgation or information disruption. Political and military maneuvering in Eastern Europe demonstrated a manner in which cyberspace can amplify political objectives through hacktivists. This study proposes that current U.S. unconventional warfare doctrine can be adapted into a model to support popular resistance, political revolution, or political reformation in and through cyberspace.

Hong Kong Protests of 2014

The recent Hong Kong protests in 2014 demonstrated principles of unconventional warfare, and are relevant to the proposed model. The following is a summary of Hong Kong protest events, particularly focusing on hacktivist activities in the cyber domain. The progression of hacktivists activities provides an indication that an unconventional warfare construct may be applicable for supporting online resistance organizations against a host nation.

Protests began following the Hong Kong Special Administrative Region handover from the United Kingdom in 1997. Among these, the principal protestations are the perennial July 1st protests, which began shortly after the handover and continue to

influence protests as recently as 2014. These annual protests underscore discontent with the handover and the dissatisfaction Hong Kong citizens have concerning the changing government. The inconsistent zeal of these protests represents the slow capitulation to the demands of the Chinese Central Government, and a potential lost opportunity for the U.S. to support a democratic people (Carroll 2007).

Hong Kong historically provides identifiable political movements that can unify some measure of its population toward a cause. For nearly two decades, protests of varying focus and size continued each year in Hong Kong, aided by what has become the July 1st effect. A demonstration of over 500,000 pro-democracy individuals was reported in 2003, protesting legislation, and ultimately forced government leaders to resign (Lee and Chan 2008, 85). The occasional successes of these protests ensure some continuation of political activist efforts each year.

More recently, the Umbrella Protests in Hong Kong in the fall of 2014 demonstrated vigorous popular dissent as thousands of students erected an encampment in downtown Hong Kong disrupting traffic, business, and government. These protests highlight both the culminating efforts of political activism and diminishment of the Hong Kong people's opportunity to resist Mainland China's expanding controls on government and the subsequent reduction of familiar freedoms enjoyed under the United Kingdom's tenure. The cause of the most recent protests stem from Mainland China's efforts to control electoral candidates for the 2017 elections by limiting candidates to those approved by Beijing (Sputnik News 2014).

In August 2014, The National People's Congress established the outline for elections in Hong Kong. These terms contrasted starkly with China's promise for

continued autonomy under handover provisions (Wall Street Journal 2014). This sudden, but perhaps inevitable, betrayal of China's policy towards Hong Kong ignited political movements among university students demanding universal (as opposed to limited) suffrage (Radio Free Asia 2015). The "Occupy Central" protests officially began at the end of September 2014, as students began civil disobedience activities in downtown areas of Hong Kong (WISHCRYS 2014).

As soon as the protests began, hacktivism developed alongside the effort to influence the Central Chinese government to rescind its suffrage-diminishing policies. On October 2, 2014, the hacktivist group Anonymous declared its support for the Occupy Central protests with online posts spread by its members and associates through various means (Jha 2014). Hong Kong protestors and hacktivists used online forums, media releases, videos, and other digital communication methods, such as pastebin(dot)com, to coordinate and discuss actions in support of the protests (Pastebin 2014).

These methods provided immediate dissemination of information and are well known to the hacker community. Anonymous used these methods to indirectly make contact with Hong Kong hacktivists in support of their cause. Information of the cyberspace attacks also reached news media outlets that reported on such activities. The hacktivists utilized legitimate discussion boards to share capabilities and coordinate offensive cyberspace operations.

The Hong Kong protests experienced a well-collaborated online effort to aid the protests and the hacktivists. A publically available Google Docs spreadsheet gave times and details of upcoming protests. Employment of hashtags was used to promote protests, and forums were used to discuss, debate, and share information for the pro-democracy

movement. A Bluetooth-based messaging app to circumvent government monitoring of Internet communications was also used to aid the cause indicating the marriage of political activism to available technology (Chu and Chan 2014). The protests aligned hacktivists under the hashtags #OpHK, #OperationHongKong, and #OpHongKong (Jha 2014). Through online posts, social media activity, videos, and media releases, the pro-Hong Kong hacktivists conveyed their objectives, unifying ideals, and how they would conduct operations to achieve their objectives.

Only when Anonymous began attacking infrastructure did the potential for rapid expansion of hacktivist capacity become apparent. Popularity of the attacks increased recruiting, aided proliferation of capabilities, and began to disrupt government networks. Online forums drew increased crowds of aspiring hacktivists, script kiddies, and the curious who desired to help the protests in anyway they could.

Despite the coordination and fervor of the Hong Kong protests, hacktivists struggled to expand their operational reach coherently, define their leadership and effectively counter the Chinese response. Thus they eventually succumbed to China's efforts to marginalize their operations. The first arrest of an individual associated with online hacktivist activity began just 10 days after Anonymous joined the cause (Radio Free Asia 2015).

One of the drawbacks of a network insurgency is the lack of leadership required to define clear goals (Patraeus and Amos 2006). This deficiency resulted in sporadic attacks that had no operational focus, either during the heightened activities in October, or during hacktivist activities that continue today. Therefore, the attacks have had only a marginal effect. The slow development of leadership has limited the ability of the

hacktivists to comprehensibly counter government reactions, likely leading to the hacktivists' culmination.

Without leadership to understand and visualize how a successful campaign might be executed, Anonymous cyberspace operations initially focused on the proverbial low-hanging fruit by attacking poorly-protected targets like the Autism Partnership website, with negligible operational or strategic effect (Moyer 2014). Anonymous frequently published their targets on various forums, to both boast of their success and to demonstrate their ability to attack Chinese government information systems. These postings were necessary as the Chinese government also muted Mainland media reporting related to the Hong Kong protests.

The initial effort of hacktivists provided little indication of coordinated attacks, or attempts at understanding the environment. However, efforts by hacktivists did expand to more effective Distributed Denial of Service attacks against public services despite failing to fully achieve a government-wide disruptive effect (Chambers 2014).

Analysis of the cyberspace operations indicates that the software used to conduct these disruptive attacks, although relatively ineffective, was simple to implement (Miu 2014). As demonstrated by the methods employed by Russian patriotic hackers, an operation can be expanded through the use of less technical tools that less technically capable individuals can deploy against a target. Use of simpler tools indicated a growing hacktivist environment within Hong Kong. Nascent hackers motivated by Occupy Central sought out hacker forums to support the struggle against the Chinese government and employed the forum-posted capabilities. Hacktivists that participated in these attacks likely experienced an increased desire for continued support for the next call to attack,

much like a conventional political activist protesting in the streets. Each successful attack increases the chance for achieving the hacktivists' ultimate goal.

The Chinese Communist Party, likely aware of the potential for protests to spread north across the Sham Chun River into the Mainland, limited media exposure of the protests in the mainland by government order. China also sought out the same forums as the hacktivists in order to disrupt or deter their growth and support. This hindered meaningful expansion of the resistance and disrupted the establishment of necessary pockets of support outside of Hong Kong (Wee 2014).

During the Hong Kong protests, some Chinese hackers assessed to be government-supported began to conduct counterattacks against Hong Kong hacktivists and related organizations (Passeri 2014). The Chinese government attacked nearly every Hong Kong-related pro-democracy website in a little over a week, and social media tags regarding the protest were blocked on Chinese networks; a few alleged supporters of Anonymous were also arrested by state police (Lam 2014).

Unprepared for this response, and unable to sustain operations, the hacktivists' efforts eventually culminated concurrently with the street protests. A few lingering attacks continued, but the effort has greatly diminished after just a few months. The hacktivists displayed some of the elementary characteristics of insurgent employment with acutely limited success. Currently, surges in effort occur every few months, but are unsustainable.

Hong Kong hacktivist efforts did successfully achieve one element of an unconventional warfare campaign by causing China to look inwards to solve their internal problems. Hong Kong hacktivists' limited ability in securing their infrastructure

exposed their weaknesses to Chinese cybersecurity efforts. The Mainland China cyber counterattacks successfully minimized any attempt by hacktivists to spread their propaganda, and thus cause any lasting effects in the cyber domain.

There were potentially a large number of hacktivists groups both inside and outside Hong Kong, operating in the current information environment to include external hacktivists organizations, such as Anonymous (Nextgov 2014). While external support is a critical element to a successful insurgency, that support must be focused on operational and strategic goals (Patraeus and Amos 2006). Even activists from Ukraine offered advice on how to resist the Hong Kong and Chinese governments (Hong 2014). However, despite the varied external support, hacktivists were unable to achieve any semblance of unity of command, and could not identify a means to attack, either directly or indirectly, the Chinese centers of gravity (Patraeus and Amos 2006). The Chinese center of gravity in this context is the Chinese Communist Party (Abernathy 2012).

By the end of October, the student protests had subsided, and protestors had generally vacated their camps. One location, Mong Kok, continued to see occasional flare-ups every few weeks following the major disbandment of protests. However, these too ultimately dwindled as the months passed. Anonymous continues to threaten the Chinese government, accusing them of various crimes, posting attacked web addresses to forums, and conducting denial of service attacks. These attacks continue sporadically; some occurred in January, and others even as late as April 2015, all under the banner of pro-Hong Kong efforts (Russon 2015). Whether uncoordinated denial of service attacks, and the occasional leaked emails are sufficient to diminish Mainland government control in Hong Kong, or influence the Communist Party to change its policies, is yet to be seen.

Validation of the Proposed Doctrinal Model Utilizing the Hong Kong Protests of 2014

The proposed model is derived from the already proven and currently employed U.S. doctrine of unconventional warfare. The discussion that follows briefly describes each phase of the proposed model, and then describes events in Hong Kong that would have occurred during each phase. Where the Hong Kong scenario is insufficient, the validation relies on the Russia-Georgia and Russia-Estonia examples discussed in Chapter 2 in order to complete a full analysis. Finally, actions that the U.S. would be expected to take in each phase (based upon the proposed unconventional warfare through cyberspace model) are offered. The results of the analysis are presented in Chapter 5, with their applicability, potential, or shortcomings reviewed.

Phase I–Preparation

Preparation provides a study and assessment of the target area, regardless of domain. During this phase, in conjunction with Military Information Support Team experts, the U.S. conducts an assessment of those online organizations that possess the capability to support the populace's anti-government movement. Many nations with an Internet capability possess dissident and opposition groups that have an online presence (Howard and Muzammil 2013). Analysis of the characteristics of these groups provides the foundation of the Preparation Phase.

Preparation must include an assessment of hacktivist activities and capabilities. The analysis necessary during this phase varies little from established protocols found in doctrinal application of unconventional warfare. Resistance groups are sought in Phase I and the focus continues in the domain within which they are active. In this case, the cyber

domain drives the requirements to identify active resistance organizations. This analysis is supported through intelligence preparation of the environment, to include new activities such as cyber intelligence preparation of the environment. The cyber domain-based unconventional warfare area of operations requires an understanding of how hacktivists shape the political environment, their level of expertise, and how their operations support major popular political causes.

The Phase I for the Hong Kong protests has a theoretically large window of opportunity. One of the first hacktivists organizations developed into a group known as the Hong Kong Blondes in the late 1990's (Hesseldahl 1998). The Preparation phase could have begun at that time; as Hong Kong began its transition to Mainland China, control and hacktivism began to take root. Phase I assessments should revolve around current issues and potential for exploitation, therefore a more concise timeline for the Preparation Phase would occur as a national issue gains popular interest. The Phase 1 assessment does not explicitly define a start since the Preparation Phase is continual. Information and intelligence assessments must constantly monitor a target nation's aptitude for a digital insurgency.

U.S. action during a Preparation Phase for the Hong Kong protests identifies those groups operating online in support of the common cause; in particular, seeking those groups that align with Combatant Command, Interagencies, and their strategic or operational goals. The culture among pro-Hong Kong hacker communities fosters the publication of their exploits in support of the protests in online forums and websites. This is the predominant way for hacktivists to promote or claim responsibility for a successful attack, and thus generate credibility among the hacker community. Additionally,

publication of the hackers' exploits allows them to increase notoriety with governing elements or the news media. This desire to publish exploits allows the U.S. to identify and classify hacktivist as potential guerillas. The analysis identifies access, technical capabilities, goals and potential influence among the population.

Phase II–Infiltration and Initial Contact

Initial contact and infiltration includes contacting resistance leadership or a government-in-exile to determine if the cause is compatible with U.S. strategic ends and if the movement is willing to accept U.S. assistance. In the cyber domain, the lines between infiltration and initial contact blur. Infiltration may occur in the cyber domain prior to initial contact as the planning and control elements conduct operational preparation of the environment and reconnaissance to establish contacts with the targeted group. Due to the virtual aspect of the domain, physical infiltration is not necessary; however, connectivity is paramount for sustained "infiltration" to both parties. This phase is a combination of Phases II and III from the original unconventional warfare doctrine.

Initial contact in the cyber domain is little different. The cyber domain provides a relatively easy means, although subject to deception, of making contact with the target organization–the Internet itself. The method may be as simple as an email, or contact through a web forum (Ottis 2011). Scores of forums exist for the sole purpose of discussing hacktivist activities, and planning the next hack. These forums are typically tiered, and require acceptance to move into the higher echelons (Meyer 1989). Regardless, proof of exploits is often a requirement for inclusion in hacker organizations. Notoriety provides the bona fides in initiating contact. The best method of approach is

beyond the scope of this study and is therefore a recommended topic for further research and discussion.

Complicating initial contact is the key element necessary for sustained cyberspace operational support to unconventional warfare–anonymity. While handles, aliases, avatars, or pseudonyms are publically displayed, the actual identities of the resistance members may be more difficult to ascertain. The legality of using unverified sources is beyond the scope of this study. The vastness in anonymity on the Internet and the lack of human contact is an obstacle to overcome in validating the identified forces. Proper preparation during Phase I can greatly increase the understanding of the environment and how to proceed to achieve successful contact. Operational security can assist in avoiding deception activities by a state's counter intelligence activities.

Hackers tend to be secretive and do not require physical interaction with the local populace for support or sustainment. These secretive organizations require a potential initiate to prove technical capability and a forum in which to publish his exploits, and to demonstrate devotion to the cause before admittance to the inner circle of a hacker cell (Meyer 1989). As demonstrated in Hong Kong, when a group with sufficient hacker-based notoriety pledges support, they are welcomed, and some coordinating efforts are accepted in order to create a larger effect against the target government.

Transition from Phase I to Phase II is at the discretion of the assessment team. For the Hong Kong scenario, this transition would occur as the assessment team determines a suitable hacktivist organization(s) to approach in support of mutual goals. This transition likely would have occurred in late September to very early October as hacktivist activities began to increase in support of the street protests. Popularity for the Hong Kong

protests began to generate considerable momentum at that time, and would present a reasonable opportunity to approach a hacktivist group to support their operations.

To conduct the infiltration with pro-Hong Kong hacktivists, the U.S. unconventional warfare control element might first engage a forum where the hacktivists meet (virtually) to discuss plans, objectives, and the relevant political issues. These members are more likely not to know the identities of forum participants, as most are anonymous (Ottis 2011a). A difficulty arises in identifying leadership as forums often form a loose network without defined leaders. Some forums are often formed around a sudden political or popular crisis.

A simple technique for initial contact and infiltration of a hacktivist group is through their nominated, or executed, targets posted to various sites, like 4chan, GitHub and others, where information on disruptive hacks, or exploits are posted. Hackers seeking to demonstrate their prowess and increase their notoriety can immediately engage the target and post their exploits. This provides a venue for the application of Phase II contact. The difficulty comes in filtering through much of the insipid inanity on such sites. Phase I analysis also provides assessments of capability, leadership, and effectiveness as well as how hacktivists are organized. The communication methods, web postings, and publications provide the analysis necessary to devise a method of contact for a successful Phase II.

Upon that initial contact, this model's Phase II requires the same rapport building as described in the parent unconventional warfare doctrine. Humans exist behind the persona, and relationship building is a critical part of any effort to develop a resistance,

irrespective of domain. Infiltration requires an understanding of the culture, jargon, and methods of communication within hacker circles to ensure success.

Phase III–Organization

Organization occurs once advisors communicate with hacktivists leaders through forums, email or message boards and the offer for support is accepted. Typical development of an organization under unconventional warfare doctrine requires rapport building and ensuring that the resistance and the U.S. share similar goals and objectives. In accordance with the originating doctrine, similar processes are followed in the organization of a resistance, whether physical or cyber-related.

Initial Organization Phase efforts emphasize training, equipping, and organizing leadership to withstand hostilities (Department of the Army 2011). Cyber resistance efforts would emphasize U.S. support to develop hacktivist infrastructure so that they could withstand state-backed surveillance attempts to defeat their cyberspace operations and communications. Network and nodal analysis enables the hacktivist to properly understand their operating environment. Without knowing the how, who and what to bring about the greatest change in the government, the cyber dissidents would become the equivalent of ordinary hacktivists, with unorganized and trendy goals. The same analysis provides an introspective look at their cybersecurity efforts and how they access the Internet. It also discerns vulnerabilities exploitable by the state security apparatus.

The Internet provides hacktivists organizational flexibility and agility unattainable in the physical domain. Internet messaging and forums enable the rapid dispersion and consolidation necessary for a cyber guerilla force to be effective (Department of the Army 2011). Without hindrance of geography, hacktivists leverage Internet infrastructure

as both lines of communication and attack vectors. Hacktivists, already established in cells, can quickly gather information on targets, obtain capabilities for the operation, disperse then attack with great rapidity (Ottis 2011a). These strengths are exploited by hacktivists for continued and future operations and increased optempo.

Any identified hacktivist organization likely comes with a pre-existing organizational hierarchy, communication methods, membership vetting processes, and concealment techniques (Gatomalo 2012; Ottis 2011). Interagency support efforts, like the physical domain, may focus on developing infrastructure such that the organization can continue to operate under increased scrutiny by a state's cybersecurity efforts. An understanding of these capabilities may also be attainable during the Preparation Phase, allowing planners to pre-position training or capabilities as the campaign progresses.

In this new domain, separate considerations for organization are necessary to ensure survival of the online resistance. Hacktivists must secure their infrastructure and establish methods for communication and security while not sacrificing flexibility and agility in cyberspace operations. When training the cyber insurgents and hacktivists, controlled U.S. cyber capabilities will likely not be shared with the dissident organization. Hacktivists who use well-worn practices, tools, and exploits to hack their way into servers and computers demonstrate the lack of immediate need for cutting-edge capabilities each day. Often the attack is as simple as a well-crafted spear phishing email, with a malicious link or attachment, waiting for the innocuous click of a mouse, whereupon the user's computer is 'owned'. These efforts are not innovative, just clever. Instructing the hacktivists, if necessary, on the proper use of available tools in a more

efficient manner mitigates much of the danger of equipping the organization with zero-day exploits; although it is wise not to entirely rule out such considerations.

Phase III of the Hong Kong hacktivist operations likely occurred around the time that Anonymous declared its intent to attack Chinese government systems. This phase would have been short-lived per the actual timeline of events, and not preferable, as the time required for Organization would likely take more than two weeks. Regardless, the declaration by Anonymous signaled a rallying of effort and coordination for attacks against the Chinese government in the cyber domain. This action increased online discussion of attacks and attack protocols in the struggle against China. These events also increased recruiting, provided a foundation of agreed upon objectives, and expectations of commitment to the cause.

The U.S. military and Interagency notionally supports the organization of a digital insurgency in Hong Kong through its analytical and cyber intelligence preparation of the environment. This information and guidance reduces the exposure of less well-connected hacktivists as they conduct their operations, allowing more focused cyberspace operations, and development of leadership, recruitment, and training for the resistance. Historically the U.S. provides surrogates support such as training, maps, imagery and other intelligence, as well as the occasional air support or radio communications equipment. This practice would continue in support of Hong Kong in this scenario, albeit through a type of support corresponding to the cyber domain.

Cyber intelligence preparation of the environment would greatly increases the effectiveness of Hong Kong hacktivist leaders and assist them in achieving their operational goals as they are aligned with U.S. strategic end states. This provides the

online resistance with targeting information that coincides with organic or U.S. provided capabilities for successful accomplishment of cyberspace attack. The sharing of information would increase the effectiveness of the hacktivists, and also enables close communication with hacktivist leadership.

In developing the digital insurgency in Hong Kong, how the U.S. supports a resistance and its limitations must be understood by the hacktivists involved. This includes applicable international laws, conventions, codes, and the prescribed rules of engagement provided through legal authorities and orders for the conduct of unconventional warfare. The U.S. must ensure that the Preparation Phase includes an analysis that clarifies the type of organization the U.S. brings that the hacktivists might be willing to accept in order to be successful in Phase III.

Phase IV–Buildup

Buildup continues, and is focused on, development of the insurgency; the intent is to expand nearly every aspect of the insurgency preparatory to the Employment Phase. Buildup is the progression of the Organization Phase, building upon the establishment of the insurgencies' capabilities so far. Doctrinally, U.S. advisors increase support through intelligence, counterintelligence, indications and warnings to the resistance group. This enables identification of confidence targets to build capacity for the resistance and further the insurgency campaign. This ensures continued development of the resistance group and avoids an unnecessary early culmination of operations if overcome by counterinsurgency operations. Progress continues much as described in the original unconventional warfare doctrine for the physical domain as it does for the cyber domain.

Phase IV activity in Hong Kong likely occurred immediately following the Organization Phase–possibly within just a few days from the start of the notional Phase III. Information systems were hacked at the same time organizational efforts of hacktivists occurred, similar to activities of a Buildup Phase. While the Buildup Phase utilizes confidence targets to build capacity, cyberspace attacks in Hong Kong during the first several days were likely used for purposes other than establishing a nascent digital insurgency. However, the effects of this phase did further consolidate efforts towards the cause. These attacks represent a hasty, self-assured effort to gain momentum and for impact against an adversary without consideration of a campaign.

Initially, limited offensive cyberspace operations build capacity. The U.S. advisory element would assist Hong Kong hacktivist leadership efforts to expand into an effective resistance by disrupting, avoiding, or circumventing, any state security apparatus and thus provide freedom of movement to the organization as they seek their goals. These initial attacks could include the disclosure of sensitive government communications, publicizing or supporting protests, phishing operations, and so forth. The U.S. would provide the analytical background to Hong Kong hacktivists as they seek to identify objectives that, once accomplished, further progress the group toward their goals and develop capacity. As the resistance organization maneuvers across the Internet with some measure of mobility and security, it can begin to transition to the Employment Phase of unconventional warfare through cyberspace.

Phase V–Employment

Hacktivists conduct offensive cyberspace operations until strategic goals are accomplished during Phase V. Combat operations include sabotage, subversion and other

disruptive attacks that constitute offensive cyberspace operations and cyberspace attack. These activities bear the same characteristics of doctrinal activities described under unconventional warfare. Operations are supported and exploited through coordination with Military Information Support Operations through the promotion of operational success (Department of the Army 2011). The Employment Phase consists of both tactical operations and psychological operations to produce the greatest effect on both the populace and the host nation as the resistance endeavors to achieve its objectives.

There is insufficient information to determine whether Hong Kong hacktivists fully entered the Employment Phase. The hacktivists, unable to fully progress through each of the preceding phases, and assess how to transition, did not experience the operational capacity enjoyed during a Phase V, and were not supported with sufficient Organization and Buildup. It may be likely that Hong Kong hacktivists attempted to immediately conduct Employment Phase-like operations, believing that a proper organizational foundation was unnecessary. Regardless, this study is unable to fully determine a timeline for a transition to the Employment Phase.

The U.S. would supports Hong Kong hacktivists by enabling repetitive attacks on varied government infrastructure. Successful attacks help hacktivists cause confusion and frustration within the targeted government. Disruptive attacks require the government to expend resources either to mitigate the effects of the attack or to disrupt hacktivist cells. Causing information security resource scarcity by attacking networks causes the government to focus inward to solve national problems and reduce external political or military efforts. This internal focus aligns with a potential U.S. strategic goal of

diminishing an adversarial state's external influence, particularly in the cyber domain, if the host nation must divert externally focused cyber capacity away from their tasks.

These conditions would further enable the U.S. to provide operational support to the digital insurgency and potentially bring the hacktivists closer to both parties' strategic goals. The U.S. would provide battle damage assessment information as well as analytical support to determine the effectiveness of the resistance's operations against the host nation. The exchange of assessments, targeting information, and indications and warnings continue until objectives are achieved. With the completion of these objectives, the military and Interagency assist the resistance to transition into the final phase of unconventional warfare.

Phase VI–Transition

The transition from an insurgency with the obtainment of objectives requires an adjustment from disruptive operations to supporting the newly established operational environment (Department of the Army 2011). During this phase, the hacktivists cease attacks and promote national security. Dangers exist that insurgents may engage in, or return to, other disputes, hacking, or criminal behavior. The new government must make an effort to assimilate these hacktivists into a positive role in support of the government, or hacktivist forces may revert to pre-insurgency status as political activists. This is perhaps the most concerning phase for planners and policy makers: a trained and organized foreign hacktivist group able to function and operate at a high skill level. Concerns and efforts remain the same between the proposed model and the principal unconventional warfare doctrine.

From the Hong Kong scenario, this study is unable to assess a Phase VI transition from the events, because it did not occur. Information on such a transition, especially in the cyber domain, is limited and incomplete. However, some consideration for the Transition Phase can be derived from separate situations involving government use of hackers.

Practical information for a Transition Phase is limited in regard to hacktivists and how the Interagency and military might proceed. However, General Keith Alexander, then Director of the National Security Agency, solicited the talents of hackers at DefCon 2012, with an undefined "all-is-forgiven" approach for reintegration into society and government employment with the hopes of avoiding hacker recidivism (Poeter 2012). The acceptance rate of that offer is unfortunately unavailable for review or analysis. If such an offer were successful, it would provide some understanding as to the feasibility of the approach.

Information following the employment of Russian patriotic hackers during the Georgia and Estonia conflicts might also provide a greater understanding for U.S. feasibility for executing a transition. However, similar to General Alexander's offer at DefCon, information and statistics are not available for additional research. These two events, however, likely hold the greatest clues as to how the U.S. might conduct Phase VI–Transition.

Validation Summary

This study proposes that current U.S. unconventional warfare doctrine can be modified and applied to support popular resistance, political revolution, or political reformation in and through cyberspace. To demonstrate the validity of the proposed

model, it was evaluated considering the events surrounding the recent Hong Kong protests in 2014. The review and comparison of doctrine and concepts to the Hong Kong protests provides the foundation for the evaluation of the proposed model as a concept for future unconventional warfare campaigns. Information was mostly available to provide an assessment for the employment of the proposed model. These conditions also represent the potential merging of current doctrine to the theoretical concept presented, which will be discussed in chapter 5.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

This study seeks to identify how the U.S. might best conduct cyberspace operations to support hacktivists and online resistance movements to exploit an adversary actor, nation, or state's weakness to achieve U.S. strategic objectives. Consideration of current doctrine and concepts of unconventional warfare and cyberspace operations provides a potential solution to determine how the U.S. might pursue national and strategic objectives through cyberspace. This chapter offers a summary of the qualitative analysis conducted in chapter 4, an interpretation of findings, and their implications regarding doctrine and future conflict. Recommendations and wider implications of this research are also presented before the chapter concludes.

Review of Model Validation

In search of a bridge over the identified gap between unconventional warfare and cyberspace operations doctrine, this study presents an operational approach for the conduct of unconventional warfare through cyberspace. Each phase of the model is assessed and validated in the context of hacktivist operations in Hong Kong and the Russian near abroad, within the scope of unconventional warfare. The modified six-phase model of this study presents a reasonable method for future unconventional warfare campaigns in the cyber domain.

Summary of Findings

This study presents unconventional warfare through cyberspace as a realistic means of employing online resistance groups as an insurgency to affect political change in adversarial governments. An analysis of each phase of the model reveals relevant artifacts in the characteristics of hacktivism necessary for an insurgency. While naturally present in most Internet-connected countries, the evidence of successful hacktivism presents itself in a chaotic manner, alluding to a requirement that planning and organization increase the chance of success. The proposed model connects the gap between how the U.S. interacts with online dissident groups and current doctrine.

Interpretation of Findings

The following discussion provides a quick definition of each phase of the proposed unconventional warfare through cyberspace model, U.S. actions during that phase according to the Hong Kong scenario, and the resulting feasibility assessment of U.S. actions for the proposed six-phased model by drawing on information presented throughout this study.

Phase I–Preparation

Preparation includes analysis and identification of resistance organizations for suitability to support U.S. objectives. This begins with the collection of relevant information while assessing the operating environment. Preparation conducted during Phase I consists of intelligence preparation of the environment and analysis of social factors. This analysis displays little difference between the cyber domain and the physical domain.

In the Hong Kong scenario, the U.S. assessment team would search for a compatible hacktivist ideology suitable for U.S. unconventional warfare efforts. Prior to and during the Hong Kong protests, sufficient information was available for the U.S. to discern hacktivist organizations' activities and efforts against the Chinese and Hong Kong governments. The cause would be readily identifiable and its popular support measurable. The U.S. would develop plans to synchronize hacktivist operations with the popular movement, and enable future disruption of government systems.

Phase I analysis using the proposed model, indicates that the doctrine may be a practical method for application in the cyber domain. The fundamental requirement for this phase is a potential or active resistance. The people of Hong Kong had psychologically prepared themselves with over a decade of protestations, suffrage issues, and unrestricted access to information, which denotes several potential resistance organizations and activities. The encroachments on the Hong Kong people's liberties by Mainland China have continued to inflame the people towards various political causes producing the hacktivists in the cyber domain necessary for unconventional warfare through cyberspace. The presence of hacktivists provides viable conditions for the Preparation Phase and further transition to Phase II.

Phase II–Infiltration and Initial Contact

Infiltration into hacktivist organizations may occur in the cyber domain prior to initial contact. The proper point of infiltration, and the method of contact, results from planning during the Preparation Phase to include reconnaissance of potential contacts within the targeted group. Contact is made through virtual connections that provide

requisite security for continued engagement. The most plausible methods are email, or contact through a web forum (Ottis 2011).

The conduct of theoretical infiltration into Hong Kong hacktivist groups stems from a thorough analysis and assessment during Phase I. The U.S. would review posted comments and recorded activities of hacktivists groups in forums and other online communication means. This analysis could identify the method, timing, and receptivity of U.S. support and aids the decision for infiltration and contact. This contact occurs electronically, either through a forum, or some other means of digital communication.

This method of contact as described in the model seems to provide a reasonable method to begin engagement of hacktivists. Exploiting the current and common methods hacktivists use to communicate with hackers, the U.S. could use these same methods for contact and infiltration. Unconventional warfare requires an understanding of the resistance organization and its cultures in order to build rapport and support. These techniques likely remain true in the cyber domain when attempting to contact a hacktivist organization. The exception to this method would be the unique instances of already knowing the identity behind a persona, and proceeding with personal engagement. Despite the possibility of internet-based communication not being exclusive, the likelihood of digital communication through hacktivist-occupied forums and websites remains the most plausible means of communicating with a hacktivist organization.

Phase III–Organization

The resistance must be organized and provided communication methods through which they may establish command and control as well as receive guidance and direction from Special Forces cyber advisors. Leadership must also be established to ensure

coordination relating to future targets and objectives. U.S. advisors must communicate capabilities and limitations as to how they can advise, train and assist the resistance in a way compatible with the resistance's goals. Through Interagency work, these requirements are developed to set the conditions for a successful resistance organization.

U.S. efforts to coordinate the development of the hacktivists during this phase would build upon the success of both Phases I and II. Developing a campaign for a nascent digital insurgency to accomplish its goals produces a greater chance of success in ensuing phases. For this purpose, unconventional warfare doctrine stresses the continuous assessment of an insurgency before advancing it to the next phase.

Hong Kong hacktivism was rushed, without centralized leadership, and efforts to organize were limited. Therefore, the scenario does not provide sufficient data for a complete analysis of expected U.S. actions in Phase III. However, Russian efforts against Georgia and Estonia can validate U.S. actions in this phase. The Russian model of support within hacker communities and hacktivists forums provides a more suitable example for success beyond Anonymous' comparative attempts in Hong Kong. The Russian example aligns well with unconventional warfare doctrine to support U.S. actions in Phase III. Russian planning prior to commencement of conventional hostilities enabled the integration of hacktivist leadership with ideology and identified objectives and targets necessary to meet Russian strategic objectives. Russian actions as described are the fundamental elements of Phase III. It is possible to assess that hacktivists' organization prior to commencement of offensive cyberspace operations, as demonstrated by Russian operations, creates the necessary command and control channels for the employment, recruitment, and establishment of hacktivists.

Phase IV–Buildup

Buildup seeks to organize the cyber guerillas, provide support through intelligence operations, and enable limited operations against targets to build confidence in the resistance. The U.S. supports this by providing cyber capabilities, training, and limited target system information to increase operational capability.

Potential U.S. assistance during the Hong Kong protests provide a rapid increase in capability, media exposure, and initial attacks on Chinese government communication systems in an attempt to further the hacktivists' cause. The introduction of an organized hacktivist system of support to lesser, ad hoc hacktivist organizations, increases the capacity and effectiveness of the resistance, at least temporarily. This environment fortifies leadership and enables the resistance to establish itself preparatory to the Employment Phase.

Assuming an appropriately timed transition from Phase III, the resistance can begin to exercise its developing capacity for future cyberspace operations. Success during the Buildup Phase should establish some centralized control or unity of command between the various hacktivist groups and initial offensive cyberspace operations. The hacktivists of Hong Kong briefly experienced the Buildup Phase, although information may be somewhat limited to achieve a full conclusion. However, drawing upon the Russia-Estonia cyberspace operations of 2007, the pro-Russian hacktivists conducted operations in a multi-phased approach, further demonstrating how the Buildup phase might occur (Conley and Gerber 2011). The first of three attacks occurred following riots in Estonia due to the Russian monument relocation, and hit various media and government websites (Traynor 2007). This attack likely validated operational methods,

and struck at a moment of popular upheaval to achieve greater effects. The pro-Russian hacktivists were then able to continue into the Employment phase over the next couple weeks once operational control and tempo could be established for future operations.

The rapidity with which both Hong Kong and Russia were able to mobilize online resistance elements indicates an untapped potential for communicating and coordinating operations necessary in the completion of the Buildup Phase. With U.S. assistance, an organized digital insurgency should see the benefit of a Buildup Phase with an established core leadership and appropriate objectives and targets suitable to achieve desired effects as capacity is tested.

Phase V–Employment

The Employment Phase sees online elements conducting cyberspace operations until the strategic end state is achieved. Operating from a solid foundation of clear and attainable objectives, organized hacktivists conduct attacks against the host nation's information systems and dominate information operations.

During Phase V the U.S. would aid the digital insurgency with target planning and execution against host nation infrastructure and other applicable objectives, improving upon the successes of the Buildup Phase. The U.S. would ensure that hacktivist cyberspace operations characterize a series of attacks representative of a planned campaign of battles, not an ad-hoc attempt at generating momentum for a cause. Coordinated and repeated attacks on varying lines of communication, infrastructure, and other high-payoff targets, frustrate and confuse host nation's efforts (Department of the Army 2011). Exploiting the weaknesses of the target government provide the lines of operation to achieve the desired end state.

The proposed model would provide the necessary guidance and assistance to a hacktivist-based insurgency during the Employment Phase through planning and intelligence support. Although the operations were short-lived, the Hong Kong hacktivists attacks represent a continued and unwitting application of doctrinal principles of unconventional warfare through cyberspace.

Again, drawing from Russian cyberspace operations against Estonia in 2007, the success of the multi-phased attacks against Estonian information systems provides some details for a proper assessment of an Employment Phase. Following the initial offensive cyberspace operations, pro-Russian hacktivist conducted two additional coordinated attacks to severely disrupt information systems. The second attack occurred during the Russian Victory Day, celebrating its victory of Germany in World War II. The third major attack occurred as President Vladimir Putin gave an aggressive speech against the Estonian government (Traynor 2007). These actions effectively punished Estonia for perceived anti-Russian behavior, and they coordinated with other political actions designed to economically injure Estonia.

Successful Russian employment of hacktivists provides the contrast to the short-lived Hong Kong online resistance and how the U.S. might support a digital insurgency. Hacktivists engaging in limited-war (cyberspace) operations with the support of U.S. intelligence, planning, and coordination are much more likely to achieve the desired strategic or military end state. The U.S. would provide operational support for a tempered, methodical, increased demand on an adversary's efforts through hacktivist cyberspace operations as described in the proposed model (Department of the Army

2011). Employment of hacktivists during Phase V would ensure that cyberspace operations persist and progress towards the desired end state.

Phase VI–Transition

In Transition, cyber guerillas are demobilized and re-assimilated as productive members of society. This important phase ensures that hacktivists do not continue to disrupt the newly established government. The purpose of transition is to return hacktivists to a pre-hostilities status, supportive of the new government in the operating environment.

The U.S. would support continued cyberspace operations until the end state is achieved and conditions are set for the Transition Phase. Following this success, the U.S. would support the new government through aiding the reintegration of hacktivists into productive roles. An understanding of individual hacktivists, their abilities, and their organizations allows for the U.S. to plan for reintegration opportunities post-conflict. The U.S. should encourage the hacktivists to support new governments, or their adaptation of controversial policies, and to cease offensive cyberspace operations, thereby enabling progress toward a secure operational environment.

Neither the Hong Kong protests nor the Russia-Georgia campaign produced evidence of a transition. Hong Kong could not successfully transition through all the phases of unconventional warfare in the cyber domain. Russian hacktivists were likely cyber criminals already in the employ of, or at least associated with, the Russian government, and therefore did not need to transition but simply resumed their prior activities (Shakarian 2011).

The potential applicability of this phase could not be assessed beyond Russian employment of cyber criminals. The only other potential aid to analysis would be the results of General Alexander's invitation to hackers to put their skills to work for the U.S. government. However, that only encompasses the U.S. population, and cannot accurately determine the behaviors of reformed hacktivist of other cultures to support government service.

This study can not conclusively assesses the model to be a valid construct for the transition of hacktivists during unconventional warfare through cyberspace due to a lack of unclassified evidence. The examples available present scattered, inconclusive information. Russia did successfully transition its conscripted hacktivists back to their prior state, regardless of what that may have been. It is also difficult to believe that General Alexander's invitation yielded zero job applications. This element of the model requires additional consideration and research to determine the best approach for the reintegration of hacktivists following an unconventional warfare campaign through cyberspace.

Implications

Campaign planning for unconventional warfare through cyberspace shares many of the same characteristics as the physical domain; success during each phase is critical for success in the next. This study indicates that the integration of cyberspace operations and unconventional warfare provide a construct suitable to wage unconventional warfare in the cyber domain. A new or diversely different doctrine is unnecessary to conduct campaign planning for unconventional warfare through cyberspace.

The findings of this study remain consistent with unconventional warfare doctrine when compared with the activities of cyber militias and hacktivists. While each phase of the proposed model could not be completely validated, this study still presents a viable step forward in advancing unconventional warfare concepts in the cyber domain. Using this model, the cyberspace operations planner has a framework to identify and develop a cyberspace unconventional warfare campaign to meet U.S. strategic goals. This model may also provide opportunities for special operations as they adapt to the cyber domain by bridging the gap where current unconventional warfare doctrine ends, and the cyber domain begins (Chairman of the Joint Chiefs of Staff 2013).

Recommendations for Further Study

Future research can build off of these concepts for full integration into a new domain of political warfare. This study examined the phased approach to unconventional warfare, specifically, those phases involved in planning a campaign. There are additional areas of research necessary for the realization of this model.

Does hacktivism inherently contain the dynamics of a successful insurgency (as described in Army Techniques Publication 3-05.1)? How would these characteristics be measured? Additional work is necessary to research the dynamics of successful insurgencies as discussed in *Special Forces Unconventional Warfare* (2011), and other publications. These dynamics vary slightly between the doctrines of counterinsurgency and support to insurgency (Chairman of the Joint Chiefs of Staff 2013). Both should be considered in future studies. Research into these dynamics and how they relate to the psychology and potential for an Internet-based insurgency would provide additional

insight during the Preparation Phase of a campaign. Such a study might improve the success of an insurgency by refining the feasibility assessment prior to start of Phase I.

How can the U.S. guide the development of resistance organizations in cyberspace? Considerable research into the composition of a cyber militia has been done (Ottis 2011b; Borowski et al. 2008; Metz 2012; Meyer 1989; Olson 2012; Ottis 2011a; Sigholm 2013; Taylor and Jordan 2004). How they are organized, recruited, sustained, and implemented is the subject of numerous studies. A link between those studies and how such an organization might operate as an insurgency within the unconventional warfare construct requires additional research. The proper development of the hacktivists during the Organization Phase ensures greater opportunities for success in later phases. Future research on this topic must coincide with the study of the dynamics of an insurgency to provide greater fidelity to assessments in Phase I.

Additional research areas may consider whether or not a government-established cyber militia can provide a suitable method for transition during the final phase of unconventional warfare. How does culture play a role for the hacktivist during Transition? How can hacktivists be reformed, reintegrated, and employed following a digital insurgency? Some research indicates that hacktivists might be recruited into a sanctioned cyber militia drawn from the public sector, much like the military reserves or a national guard (Applegate 2011). While the aforementioned research did not consider development of a cyber militia post-conflict (i.e. Transition Phase), it develops the idea of how to employ hackers and hacktivists in support of the government–a critical element because the realization of unconventional warfare requires a model for its final phase. The analysis conducted in this research was unable to fully determine the applicability of

the proposed model during Phase IV Buildup. A study of the cultures of these secretive organizations and their government interaction may be difficult, but could yield the answers necessary for a successful transition to the final phase of an insurgency in each operational environment.

Under what timeline are insurgencies in the cyber domain more likely to find success? Another issue requiring future research is to determine whether a protracted cyberspace insurgency is more beneficial to the resistance, or to the enemy. Historically, protracted insurgencies provided greater chances of survival by avoiding decisive engagement with the dominant governing force (Stewart 2012). Limiting engagement and selective loss of ground helps the ground insurgency maintain combat power, and provides the opportunity to regroup at another time and location of its choosing. In the study of an insurgency conducted through cyberspace, one must ask whether protracted engagements still benefit the insurgent. The enemy owns all the terrain–the Internet Service Providers, local infrastructure, state security apparatus, etc. The enemy is therefore able to observe, record, and research each action of the digital insurgent either during or after each attack. Much like antivirus companies, nations can build countermeasures and filters to the insurgent's essential tactics as the resistance endures. Future research may answer how a protracted insurgency may or may not be of benefit in the cyber domain.

Additionally, what does success look like in a digital insurgency? Is an online resistance organization expected to completely overthrow a government, or does it only need to affect change in policies governing the free flow of information? The measures of success for a digital insurgency demand the necessary planning and consideration on how

to determine the effectiveness of an insurgency in the cyber domain. An understanding of the expectations of the resistance can enable decisions for phase transitions and how well objectives are met. Future research must ask how tactical actions translate into strategic objectives, and demonstrate measurement of these gains.

How does the U.S. operate with unverifiable resistance leadership in pursuit of a digital insurgency? Attainment of authorities to conduct an unconventional warfare campaign through cyberspace likely requires considerable review and discussion between the Interagency, Combatant Commanders and the Joint Chiefs. Additionally, in the course of developing an online insurgency, it is foreseeable that the identities of the hacktivists may not be immediately ascertained. In such instances, the legality of using unverified sources to engage in unconventional warfare in the cyber domain needs further elaboration and definition.

Summary and Conclusions

Unconventional warfare in the cyber domain is feasible. The U.S. military and Interagency must study, develop, and apply policies that utilize both the military and social aspects of cyberspace to achieve strategic goals. The combination of both of these factors holds a construct that amplifies the effects of cyberspace operations. Unconventional warfare through cyberspace provides the way to bridge the gap linking modern concepts of war in the cyber domain to current U.S. doctrine. The means of unconventional warfare change with the passage of time, yet its principles remain consistent, requiring continued adaptation to current and future threats in the cyber domain. This study demonstrates the potential for an unconventional warfare campaign

following a recommended cyberspace model that the U.S. must use or risk falling behind the innovations of her competitors.

Political movements carry similar traits regardless of domain; therefore unconventional warfare doctrine has relevance in the cyber domain. Clausewitz said, "the passions that are to be kindled in war must already be inherent in the people" (Howard, Paret and West 1984). The existence of hacktivism represents that passion that must be kindled for resistance. The U.S. cannot disregard social movements occurring in cyberspace as simple trends, but must find ways to kindle resistance against oppressive regimes to aid in securing strategic objectives.

No major retooling of established doctrine is necessary to adopt the proposed model. Unconventional warfare in the cyber domain is plausible, and should be used to disrupt adversarial governments and deter aggression and intellectual property theft. The decreasing size of the U.S. Armed Forces requires innovative ideas to meet strategic objectives without incurring additional costs in all domains. Currently, near-peer states are enhancing their doctrine to include full utilization of cyberspace in support of their elements of national power. The U.S. possesses a seemingly dormant doctrine that provides a solution to strategic concerns if applied.

Unclassified U.S. cyber policy explicitly states the cyber threat from countries like Iran, Russia, China, and North Korea are of the greatest concern (Department of Defense 2015). Most of these countries contain online elements either actively or covertly resisting its government, as well as supporting it. Support to a digital insurgency may reduce the threat described in Department of Defense policy as these countries are forced to look inward to manage internal problems caused by an insurgency. The joint

planner can realize the effects of tactical actions in support of attaining strategic objectives through unconventional warfare in the cyber domain.

Cyberspace unconventional warfare utilizes hacktivists whose digital personas operate within the cyber domain as the cyber insurgent or cyber militia to achieve strategic objectives. This focus evolves planning from a tendency towards capabilities-based planning, and returns to effects-based planning. Hacktivists personify offensive cyberspace operations and cyberspace attack causing the target nation to refocus its resources and efforts inward to fight a digital insurgency. The relevancy of unconventional warfare doctrine has never been so apparent as it is in today's connected world. The U.S. must seek out and organize online resistance organizations using the principles of unconventional warfare in order to counter the threat from nations who are themselves vulnerable to the chaos and disorder of a digital insurgency.

REFERENCE LIST

Abernathy, James T. 2012. "The Chinese Communist Party: A Strategic Center of Gravity Analysis." Strategy Research Project, Army War College.

Abidin, Cristal. 2014. "An Organic #OccupyCentral TimeLine on-site at Admiralty." WISHCRYS. Accessed May 1, 2015. http://wishcrys.com/2014/11/24/an-organic-occupycentral-timeline-on-site-at-admiralty/.

Applegate, Scott. 2011. "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security and Privacy* 9, no. 5: 16-22.

Ashmore, William C. 2009. "Impact of Alleged Russian Cyber Attacks." Monograph, School of Advanced Military Studies, Fort Leavenworth.

Baase, Sara. 2008. *A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet*. Upper Saddle River, NJ: Pearson Prentice Hall.

Bamman, David, Brendan O'Connor, and Noah Smith. 2012. "Censorship and Deletion Practices in Chinese Social Media." *First Monday* 17, no. 3. Accessed January 1, 2015. http://www.ojphi.org/ojs/index.php/fm/article/view/3943/3169.

Basilaia, Mikheil. 2012. "Volunteers and Cyber Security: Options for Georgia." Master's thesis, Tallinn University of Technology.

Baumann, Robert F. 1997. "Historical Perspectives on Future War." *Military Review* 77 no. 40 (March-April): 46.

Borowski, Kyle, Bettine Hunterburg, Brian Malloy, Mark Matulka, Nancy McGauvran, Kristin Phaneuf, and Amber Wolf. 2008. *Cyber Militias*. Omaha, NE: U.S. Strategic Command.

Bradner, Eric. 2014. "Obama: North Korea's Hack not a War, but 'Cybervandalism'." CNN, December 21. Accessed January 2, 2015. http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/.

Bumgarner, John, and Scott Borg. 2008. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." U.S. Cyber Consequences Unit. Registan. Accessed June 6, 2015. http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

Carr, Jeffrey. 2010. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media.

Carroll, John M. 2007. *A Concise History of Hong Kong*. Lanham, MD: Rowman and Littlefield.

Chairman of the Joint Chiefs of Staff. 2014. Joint Publication 3-05, *Special Operations*. Washington DC: Department of Defense.

———. 2013. Joint Publication 3-12(R), *Cyberspace Operations*. Washington DC: Department of Defense.

Chambers, Joshua. 2014. "Exclusive: Victor Lam, Deputy CIO on Coping with Hacktivist Attacks." FutureGov. Accessed February 14, 2015. http://futuregov.epublishing.com/articles/5278-exclusive-victor-lam-deputy-gcio-on-coping-with-hacktivist-attacks.

Chang, Amy. 2014. "Warring State: China's Cybersecurity Strategy." Center for a New American Security, December 3. Accessed December 20, 2014. http://www.cnas.org/chinas-cybersecurity-strategy.

Chu, Jeff, and Chan, Helsa. 2014. "5 Ways Protestors Organized #OCCUPYCENTRAL." Fast Company. Accessed February 15, 2015. http://www.fastcompany.com/3036374/5-ways-protesters-organized-occupycentral.

Clarke, Richard A. 2010. *Cyber War*. New York, NY: Harper-Collins Publishers.

Conley, Heather A., and Theodore P. Gerber. 2011. *Russian Soft Power in the 21st Century: An Examination of Russian Compatriot Policy in Estonia*. Washington, DC: Center for Strategic and International Studies.

Department of Defense. 2015. *The Department of Defense Cyber Strategy*. Washington, DC: Department of Defense.

Department of Homeland Security. 2011. "DHS Bulletin: Anonymous/LulzSec Has Continued Success Using Rudimentary Hacking Methods." Public Intelligence. Accessed December 15, 2014. https://publicintelligence.net/dhs-bulletin-anonymouslulzsec-has-continued-success-using-rudimentary-hacking-methods/.

Department of the Army. 2011. Training Circular 18-01, *Special Forces Unconventional Warfare*. Washington, DC: Department of the Army.

———. 2003. Field Manual 3-05.130, *Army Special Operations Forces Unconventional Warfare*. Washington, DC: Department of Defense.

Eidman, Christopher R., and Gregory Green Scott. 2014. "Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Warfare." Master's thesis, Naval Postgraduate School.

Estes, Adam C. 2014. "Why Sony Keeps Getting Hacked." Gizmodo. Accessed December 9, 2014. http://gizmodo.com/why-sony-keeps-getting-hacked-1667259233.

Galula, David. 2006. *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praeger Security International.

Gatomalo. 2012. "Cyber Militia Models-Offensive." US Cyber Labs. Accessed September 30, 2014. http://uscyberlabs.com/blog/2012/02/15/cyber-militia-models-offensive/.

Ghannam, Jeffery. 2011. *Social Media in the Arab World: Leading up to the Uprisings of 2011*. Washington, DC: The Center for International Media Assistance.

Gill, Stephen. 2000. "Toward a Postmodern Prince? The Battle in Seattle as a Moment in the New Politics of Globalisation." *Journal of International Studies* 29, no. 1: 131-140.

Hansen, Evan. 2010. "Why WIKILEAKS is Good for America." Wired. Accessed September 30, 2014. http://www.wired.com/2010/12/wikileaks-editorial/.

Hesseldahl, Arik. 1998. "Hacking for Human Rights?" Wired. Accessed May 8, 2015. http://archive.wired.com/politics/law/news/1998/07/13693.

Hong, Brendan. 2014. "China's Internet is Freer than You Think." The Daily Beast. Accessed May 1, 2015. http://www.thedailybeast.com/articles/2014/12/27/china-s-internet-is-freer-than-you-think.html.

Howard, Michael, Peter Paret, and Rosalie West. 1984. *Carl Von Clausewitz: On War.* Princeton, NJ: Princeton University Press.

Howard, Philip N., and Muzammil M. Hussain. 2013. *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. New York, NY: Oxford University Press.

Jha, Abhishek K. 2014. "#OpHK aka Operation Hong Kong: Anonymous Hacks Chinese Government Website." Techworm. Accessed January 10, 2015. http://www.techworm.net/2014/10/operation-hong-kong-anonymous-hacks-chinese-government-website.html.

Kaufman, Sarah. 2014. "Hong Kong Protesters' Phones Hit by iOS Virus." Vocativ. Accessed October 30, 2014. http://www.vocativ.com/world/china/hong-kong-protesters-virus/.

KGS NightWatch. 2011. "For the Night of 17 January 2011." KForceGov. Accessed January 17, 2011. http://www.kforcegov.com/services/is/NightWatch/NightWatch_11000013.aspx.

Klimburg, Alexander. 2010. "The Whole of Nation of Cyberpower." *Geographic Journal of International Affairs* 11: 175.

Knapp Jr, Everett D. 2012. “Unconventional Warfare in Cyberspace.” Strategic Research Project, Army War College.

Knox, Williamson, and MacGregor Murray. 2001. *The Dynamics of Military Revolution, 1200-2050*. New York, NY: Cambridge University Press.

Kopstein, Joshua. 2014. “How the NSA Recruits in a Post-Snowden World.” The Daily Beast. Accessed May 6, 2015. http://www.thedailybeast.com/articles/2014/01/17/how-the-nsa-recruits-in-a-post-snowden-world.html.

Koyfman, Tanya. 2014. “Ukraine versus Russia in a Cyber-Duel.” SenseCy. Accessed October 20, 2014. http://blog.sensecy.com/2014/03/03/ukraine-versus-russia-in-a-cyber-duel/.

Lam, Oiwan. 2014. “The Invisible Violence of Cyber War in Hong Kong’s Umbrella Revolution.” Global Voices Online. Accessed February 16, 2015. http://advocacy.globalvoicesonline.org/2014/10/06/the-invisible-violence-of-cyber-war-in-hong-kongs-umbrella-revolution/.

Lee, Francis L., and Joseph M. Chan. 2008. “Making Sense of Participation: The Political Culture of Pro-democracy Demonstrators in Hong Kong.” *The China Quarterly*, no. 193 (March): 84-101. http://dx.doi.org/10.1017/S0305741008000052.

Lin, Herbert. 2012. “Cyber Conflict and International Humanitarian Law.” *International Review of the Red Cross* 94, no. 886: 515-531.

Metz, Stephen. 2012. “The Internet, New Media, and the Evolution of Insurgency.” Strategic Research Project, U.S. Army War College.

Meyer, Gordon R. 1989. *The Social Organization of the Computer Underground*. De Kalb, IL: Northern University of De Kalb.

Mills, Elinor. 2012. “Old-Time Hacktivists: Anonymous, You’ve Crossed The Line.” CNet. Accessed February 14, 2015. http://www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line/.

Miu, Tony. 2014. “Network Threats and Attacks Analysis.” MiuTony. Accessed February 14, 2015. http://miutony.blogspot.hk/2014/10/analysis-of-cyber-warfare-weapons-on.html.

Moyer, Justin. 2014. “Report: Hacker Collective Anonymous Joins Hong Kong’s Occupy Central.” *The Washington Post*. Accessed February 14, 2015. http://www.washingtonpost.com/news/morning-mix/wp/2014/10/02/report-anonymous-hacker-collective-joins-hong-kongs-occupy-central/.

Mumford, Andrew. 2013. *Proxy Warfare*. Maiden, MA: Polity Press.

Nakashima, Ellen, and Joby Warrick. 2012. “Stuxnet was Work of U.S. and Israeli Experts, Officials Say.” *The Washington Post*. Accessed January 2, 2015. http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

NextGov. 2014. “Hacktivists Back Hong Kong’s Occupy Central.” NextGov. Accessed February 14, 2015. http://www.nextgov.com/cybersecurity/2014/10/hacktivists-back-hong-kongs-occupy-central/95711/.

Norris, Pip. 2007. “Political Activism: New Challenges, New Opportunities.” In *Oxford Handbook of Comparative Politics*, edited by Carles Boix and Susan C. Stokes, 628-652. New York, NY: Oxford University Press.

Office of the Press Secretary. 2014. “Readout of National Security Advisor Susan E. Rice’s Meeting with Foreign Minister Wang Yi of China.” Whitehouse.gov. Accessed February 25, 2015. https://www.whitehouse.gov/the-press-office/2014/10/01/readout-national-security-advisor-susan-e-rice-s-meeting-foreign-ministe.

Olson, Parmy. 2012. *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York, NY: Little, Brown and Co.

Ottis, Rain. 2011a. *A Systematic Approach to Offensive Volunteer Cyber Militia*. Tallinn, Estonia: TUT Press.

———. 2011b. “Theoretical Offensive Cyber Militia Models.” Paper presented at Proceedings of the International Conference on Information Warfare, Washington, DC, March 17-18.

Parker, Kevin L. 2014. “The Utility of Cyberpower.” *Military Review* 92, no. 3 (May-June): 26-33.

Passeri, Paolo. 2014. “1-15 October 2014 Cyber Attacks Timeline.” Hackmageddon. Accessed February 16, 2015. http://hackmageddon.com/2014/10/20/1-15-october-2015-cyber-attacks-timeline/.

Pastebin. 2014. “#OpHK.” Accessed April 1, 2015. http://pastebin.com/99524WpV.

Patraeus, David H., and James F. Amos. 2006. Field Manual 3-24 *Counterinsurgency*. Washington, DC: Department of the Army.

Poeter, Damon. 2012. “DefCon: NSA Boss Asks Hackers to Join the Dark Side.” PC Mag. Accessed February 16, 2015. http://www.pcmag.com/article2/0,2817,2407783,00.asp.

Poulsen, Kevin. 2015. “Surprise! America Already Has A Manhattan Project For Developing Cyber Attacks.” Wired. Accessed February 19, 2015. http://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/.

Radio Free Asia. 2015. “Umbrella Timeline.” Radio Free Asia. Accessed May 1, 2015. http://www.rfa.org/english/multimedia/timeline/UmbrellaTimeline.html.

Rantapelkonen, Jari, and Mirva Salminen. 2013. *The Fog of Cyber Defense*. Helsinki, Finland: National Defense University/Department of Leadership and Military Pedagogy.

Reagan, Ronald. 1986. “Radio Address to the Nation on Terrorism.” University of California Santa Barbara. Accessed December 12, 2014. http://www.presidency.ucsb.edu/ws/?pid=37376.

Russon, Mary-Ann. 2015. “Anonymous Brings Down 30 Chinese Government Websites to support Hong Kong Protestors.” International Business Times. Accessed April 13, 2015. http://www.ibtimes.co.uk/anonymous-brings-down-30-chinese-government-websites-support-hong-kong-protesters-1496069.

Savov, Vlad. 2014. “Sony Pictures Hacked: The Full Story.” The Verge. Accessed December 8, 2014. http://www.theverge.com/2014/12/8/7352581/sony-pictures-hacked-storystream.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, NY: Cambridge University Press.

Security Ninja. 2011. “Share Prices and Data Breaches.” Security Ninja. Accessed December 9, 2014. http://www.securityninja.co.uk/data-loss/share-prices-and-data-breaches/.

Shakarian, Paolo. 2011. “The 2008 Russian Cyber Campaign Against Georgia.” *Military Review* 91, no. 6: 63.

Sigholm, Johan. 2013. “Non-State Actors in Cyberspace Operations.” *Journal of Military Studies* 4, no. 1: 2-10.

Sputnik News. 2014. “Anonymous Hacktivist Group Declares War against Hong Kong Authorities.” Sputnik News. Accessed May 1, 2015. http://sputniknews.com/world/20141002/193556955.html.

Sterling, Bruce. 2014. *The Hacker Crackdown, Law and Order on the Electronic Frontier*. New York, NY: Bantam Books.

Stewart, Scott. 2012. “Insurgency and the Protracted War.” StratFor. Accessed April 19, 2015. https://www.stratfor.com/weekly/insurgency-and-protracted-war.

Stuart, Hunter. 2014. "Americans Fear Hacking More Than Any Other Crime, Poll Finds." *The Huffington Post*. Accessed November 3, 2014. http://www.huffingtonpost.com/2014/10/28/hacking-fear-poll_n_6057100.html.

Taylor, Paul A., and Tim Jordan. 2004. *Hacktivism and Cyberwars: Rebels with a Cause* New York, NY: Psychology Press.

The Armed Forces Communications and Electronics Association International. 2012. "Overview of the Russo-Georgian War (2008)." AFCEA. Accessed November 13, 2014. http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

Traynor, Ian. 2007. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*. Accessed May 23, 2015. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

Tsang, Emily. 2014. "11 Arrested over Cyberattacks on 70 Government Websites." *South China Morning Post*. Accessed October 22, 2015. http://www.scmp.com/news/hong-kong/article/1622171/more-70-hong-kong-government-websites-under-attack-anonymous-hackers.

Valacich, Joseph, and Christopher Schneider. 2012. *Information Systems Today*. Upper Saddle River, NJ: Prentice Hall.

Wall Street Journal. 2014. "China's 'One Country, Two Systems' Trap." *The Wall Street Journal*. Accessed May 1, 2015. http://www.wsj.com/articles/SB10001424052702304914204579394311122259036.

Wee, Sui-Lee. 2014. "HK Protests' 'Umbrella Revolution' Tag Escapes China's Sensors-So Far." The Daily Mail. Accessed February 16, 2015. http://www.dailymail.co.uk/wires/reuters/article-2774563/HK-protests-Umbrella-Revolution-tag-escapes-Chinas-censors--far.html.

Williams, Brett T. 2014. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly* 73: 12-19.

Wong, Scott. 2012. "Joseph Kony Captures Congress' Attention." Politico. Accessed February 14, 2015. http://www.politico.com/news/stories/0312/74355.html.

Yahoo. 2014. "Recruiting Hackers." Yahoo News. Accessed October 13, 2014. http://news.yahoo.com/video/recruiting-hackers-091642049.html.